《붉은별》 봉사기용체계 3.0
기초보안설정지도서

차 례

1. root 통과암호에 대한 요구사항 1
2. 체계관리자와 보안관리자권한.... 1
3. 중요한 체계화일들의 권한과 속성에 의한 보안실현.... 3
4. 중요한 체계화일들을 압축보관.... 6
5. 체계디스크와 자료디스크구분에 의한 자료보안실현 6
6. 여벌복사를 다른 디스크에 진행하는 방법 6
7. root 의 crontab 국부여벌복사설정으로 자료대피 7
8. etc/xinetd.d/의 불필요한 봉사화일의 뒤문없애기.... 8
9. etc/rc.d/init.d/불필요한 초기화화일들을 삭제 8
10. etc/services 에서 사용하지 않는 포구정보설명처리 8
11. /etc/hosts.allow, /etc/hosts.deny 화일에서 접근허용설정 8
12. 규정위반사용자식별자특별관리 9
13. root 권한으로 체계에 가입하는것은 보안상위법행위 10
14. 같은 종류의 프로쎄스 한번에 모두 끄기.... 11
15. ping 에 응답하지 않게 설정하는 보안.... 12
16. Root 소유의 SetUID, SetGID 화일 조사 12
17. su 지령사용만을 확인하는 방법 14
18. 기본실행되는 불필요한 프로쎄스제거 15
19. /etc/rc.d/rc.local 화일에 기동시에 기동할 화일등록 16
20. 화일과 디스크보안을 위한 방법들.... 16
21. SetUID, SetGID, StickyBit 설정 18
22. 원격봉사기의 사용자식별자정보확인.... 21
23. 봉사기부하률을 통한 보안점검.... 22
24. 보안을 위한 find 활용 23
25. 화일속성으로 화일보안실현.... 28
26. 하드디스크의 물리적인 고장발생과 대책 32
27. 화일을 삭제하지 않고 용량만 0 으로 설정.... 35
28. 디스크사용량점검지령 du.... 35
29. 화일체계별 디스크사용량을 점검하는 df 지령.... 37
30. 화일의 소유자와 그룹변경지령 chown.... 40
31. 화일권한을 설정하는 chmod 지령 43
32. 망보안주사도구 nmap.... 47
33. 망지령들에 대한 사용법은 보안의 힘있는 도구 49
34. tcpdump 를 리용한 TCP 파케트수집 및 파케트자료관리 56
35. 마지막 등록가입접속확인.... 59

36. 여벌복사봉사기구축 62

위대한 령도자 **김정일**동지께서는 다음과 같이 지적하시였습니다.

《프로그람을 개발하는데서 기본은 우리 식의 프로그람을 개발하는것입니다. 우리는 우리 식의 프로그람을 개발하는 방향으로 나가야 합니다.》

(《**김정일**선집》 제15권, 196페지)

봉사기관리자의 역할에 대하여 지금까지 그 어떤 도서에서도 강조된것이 없습니다. 그러면 봉사기관리자의 역할이 어떤 문제인가를 설명할 필요가 있습니다. 더우기 오늘과 같이 세계적인 싸이버전이 시작된 시점에서 봉사기관리자들이 이에 대처하여 자기들의 봉사기들을 보호하고 운영을 유지하는 문제는 단순히 기술실무적인 문제가 아니라는것은 명백합니다.

여기서는 봉사기관리자들이 초보적으로 알아야 할 보안설정부분을 설명합니다.

1. root 통과암호에 대한 요구사항

① 통과암호는 최소한 8 문자이상이여야 합니다.

② 수자와 문자가 반드시 결합되여야 합니다. 그래야 통과암호해득프로그람이 통과암호를 해득하는 시간을 늘일수가 있습니다. 보통 8 자리 수자만으로 이루어진 통과암호는 통과암호해득프로그람이 6 시간이면 풀어낸다. 8 개의 문자로만 이루어져있는 통과암호는 48 시간이면 풀어낸다. 문자, 수자가 결합된 8 문자의 통과암호는 석달이상이 걸립니다.

③ 한달에 한번씩 통과암호를 바꾸어야 합니다.

④ 통과암호를 종이에 적어서 보관하는 현상을 없애야 합니다.

⑤ 통과암호를 작성할 때 어떤 지명이나 이름, 생년월일등을 피해야 하며 사전에 없는 문자들로 구성해야 합니다.

2. 체계관리자와 보안관리자권한

《붉은별》봉사기용체계 3.0 에서는 보안의 중요성으로부터 체계관리자와 보안관리자라는 개념을 도입하였습니다.

《붉은별》봉사기용체계 3.0 를 설치할 때 root 통과암호를 설정하게 됩니다. 이 통과암호는 관리자권한을 제한한 통과암호로서 이 통과암호로 체계에 가입하면 체계설정과 관련한 조작만을 진행할수 있습니다. 즉 보안관련설정은 진행할수 없습니다.

설치를 끝내고 체계를 처음 기동한 다음 사용자이름(root)과 그 사용자의 통과암호를 입력하여 체계에 가입합니다.

```
《붉은별》봉사기용체계 3.0판
핵심부 2.6.32-201305.RSS3.i686 (i686)
localhost login: root
Password:
Last login: Fri May 31 10:27:14 on tty2
[root@localhost ~]# id -Z
root:sysadm_r:sysadm_t:s0-s15:c0.c1023
[root@localhost ~]#
```

우의 화면에서는 root사용자로 체계에 가입하였을 때 그 사용자의 권한이 체계관리자라는것을 보여줍니다. id –Z지령은 체계관리자의 보안문맥정보를 보여줍니다.

체계관리자권한으로부터 보안관리자권한을 얻자면 다음과 같은 지령들을 실행시켜야 합니다.

```
《붉은별》봉사기용체계 3.0판
핵심부 2.6.32-201305.RSS3.i686 (i686)
localhost login: root
Password:
Last login: Fri May 31 10:27:14 on tty2
[root@localhost ~]# id -Z
root:sysadm_r:sysadm_t:s0-s15:c0.c1023
[root@localhost ~]# sadm -s
암호화일을 창조합니다...
........................
새 암호 :
암호 확인 :
암호가 설정되였습니다!
[root@localhost ~]# sadm -r secadm_r
보안관리자암호 :
................가입...........
암호:
[root@localhost ~]# id -Z
root:secadm_r:secadm_t:s0-s15:c0.c1023
[root@localhost ~]# _
```

체계설치후 보안관리자의 암호는 기정으로 설정되여있지 않습니다. 따라서 보안관리자권한을 얻자면 먼저 보안관리자의 암호를 설정하여야 합니다.

sadm –s지령은 보안관리자의 암호를 설정하는 지령입니다.

보안관리자의 암호를 설정한 다음 sadm –r secadm_r 지령을 리용하여 보안관리자권한을 얻을수 있습니다. 이때 보안관리자의 암호와 체계관리자의 암호가 정확히 입력되여야만 보안관리자권한을 얻을수 있습니다.

id –Z 지령을 통하여 보안관리자의 문맥을 확인합니다.

보안관리자권한으로는 보안조작체계설정을 비활성화할수 있습니다. 보안조작체계설정을 비활성화하는 경우 체계의 보안을 담보할수 없으므로 이와 같은 설정은 특별한 경우를 제외하고는 사용하지 말아야 합니다.

```
[root@localhost ~]# id -Z
root:secadm_r:secadm_t:s0-s15:c0.c1023
[root@localhost ~]# setenforce 0
[root@localhost ~]# getenforce
Permissive
[root@localhost ~]# _
```

여기서 setenforce 0은 보안조작체계를 비활성화하는 지령이고 getenforce지령은 보안조작체계가 비활성화되였는가를 확인하는 지령입니다. permissive는 보안조작체계가 비활성화되였다는것을 의미합니다.

보안조작체계를 다시 활성화하자면 다음의 지령을 실행하면 됩니다.

```
[root@localhost ~]# setenforce 1
[root@localhost ~]# getenforce
Enforcing
[root@localhost ~]#
```

여기서 enforcing 은 현재 보안조작체계가 활성화되였다는것을 보여줍니다.

보안《붉은별》봉사기용체계 3.0 설정상태에서 탈퇴하자면 즉 초기가입상태로 되돌아가자면 다음의 지령을 실행합니다.

```
[root@localhost ~]# exit
가입탈퇴
[root@localhost ~]# id -Z
root:sysadm_r:sysadm_t:s0-s15:c0.c1023
[root@localhost ~]# _
```

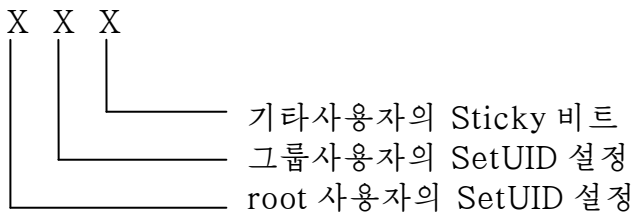
3. 중요한 체계화일들의 권한과 속성에 의한 보안실현

봉사기설치직후에 중요한 체계화일들에 대한 권한과 속성들을 재설정해야 합니다. 이것은 해커가 화일을 수정하려고 할 때 그렇게 되지 못하도록 설정하기 위해서입니다. 이 화일들에 권한을 최대제한조건(관리자만 실행하려면 100 권한)로 설정하고 화일이 수정되지 않도록 가장 강력한 화일속성인 i 속성을 부여해야 합니다.

먼저 su지령을 비롯한 중요한 관리자지령들의 사용을 제한하는 설정을 봅시다.

su지령은 일반사용자들이 사용하는 경우가 극히 적으므로 가능하다면 관리자들만이 사용하도록 설정합니다. 례를 들어 wheel라는 관리자그룹에 소속된 사용자들만이 이 지령을 사용하도록 하려면 다음과 같이 합니다.

```
# chmod  4750 /bin/su
#chown  root:wheel  /bin/su
#chattr  +i  /bin/su
```

첫번째설정은 /bin/su의 권한을 4750으로 설정하였습니다. 첫번째설정의 4번째수자의 의미는 다음과 같습니다.

해당 비트가 1이면 설정이고 0이면 비설정입니다.

4는 root사용자의 SetUID비트를 설정한것으로서 이렇게 설정된 지령이 실행될 때는 root사용자권한을 실행하게 됩니다. 이 수자가 2일때 그룹사용자의 SetUID비트이고 1일때 기타사용자의 Sticky비트설정입니다. 둘째수자설정에서 7은 root에게 모든 권한을 주는것이고 셋째수자설정에서 5는 그룹사용자에게 읽기와 실행권한을, 넷째수자설정에서 0은 기타 다른 사용자들에게는 그 어떤 권한도 주지 않는다는 의미입니다.

두번째설정은 /bin/su의 소유자를 root로 설정하고 그룹의 소유자를 wheel로 설정한것입니다.

세번째설정은 /bin/su화일에 대한 i속성을 부여한것입니다. 이것은 이 화일에 대한 수정 또는 삭제가 되지 않도록 설정한것입니다.

```
[root@dell-rss home]# chmod 4750 /bin/su
[root@dell-rss home]# chown root:wheel /bin/su
[root@dell-rss home]# chattr +i /bin/su
[root@dell-rss home]# ls -l /bin/su
-rwxr-x---  1 root wheel 52810  2007  4월 13 06:52 /bin/su
[root@dell-rss home]# lsattr /bin/su

----i-------- /bin/su
[root@dell-rss home]#
```

즉 이렇게 등록하면 wheel 그룹에 등록된 사용자들만 su 지령을 사용할수 있습니다. 따라서 su 지령을 허용할 사용자들을 /etc/group 화일의 wheel 그룹에 등록해 주면 됩니다. Vi 편집지를 열어서 다음과 같은 내용을 추가합니다.

#wheel:x:10:root

대부분 wheel 그룹에 등록된 사용자들은 봉사기관리자나 특정권한을 가지는 사용자입니다. 이와 같이 《붉은별》봉사기용체계 3.0 에서 다른 모든 지령들의 설정을 이와 같은 방법으로 하면 됩니다. 례를들어 /usr/sbin/usradd 나 /usr/sbin/top, /sbin/fdisk, /sbin/mkfs, /sbin/fsck 들과 같이 주로 체계관리자들만 사용하는 지령들을 모두 이와 같은 방법으로 설정할수 있습니다.

다음은 5 개의 지령들에 대하여 wheel 그룹에 소속된 사용자들만 사용할수 있도록 설정한것입니다.

먼저 권한설정을 봅시다. 앞의 실례에서 /bin/su 는 SetUID 가 설정되여 있어야 하지만 이런 일반적인 관리자지령에는 SetUID 가 설정되여 있지 않아도 상관없기때문에 모두 750 으로 설정합니다.

```
[root@dell-rss home]# chmod 750 /usr/sbin/useradd
[root@dell-rss home]# chmod 750 /usr/bin/top
[root@dell-rss home]# chmod 750 /sbin/fdisk
[root@dell-rss home]# chmod 750 /sbin/mkfs
[root@dell-rss home]# chmod 750 /sbin/fsck
[root@dell-rss home]#
```

다음은 소유자와 그룹을 설정한것입니다.

```
[root@dell-rss home]# chown root:wheel /usr/sbin/useradd
[root@dell-rss home]# chown root:wheel /usr/bin/top
[root@dell-rss home]# chown root:wheel /sbin/fdisk
[root@dell-rss home]# chown root:wheel /sbin/mkfs
[root@dell-rss home]# chown root:wheel /sbin/fsck
[root@dell-rss home]#
```

그리고 다음은 삭제와 변경이 되지 않도록 하기 위하여 i속성을 부여한것입니다.

```
[root@dell-rss home]# chattr +i /usr/sbin/useradd
[root@dell-rss home]# chattr +i /usr/bin/top
[root@dell-rss home]# chattr +i /sbin/fdisk
[root@dell-rss home]# chattr +i /sbin/mkfs
[root@dell-rss home]# chattr +i /sbin/fsck
[root@dell-rss home]# █
```

여기서는 5개의 지령들만 실례를 들어 설명했지만 《붉은별》봉사기용체계 3.0체계에서는 일반사용자들이 사용할 필요가 없는 관리자지령들이 많습니다.

4. 중요한 체계화일들을 압축보관

《붉은별》봉사기용체계 3.0에는 중요한 체계화일임과 동시에 자주 해킹표적으로 되는 체계화일들이 많이 있습니다. 이 화일들은 체계가 해킹된 후에는 거의 대부분 수정되여 관리자가 체계상태를 정확하게 파악할수 없도록 만들어 버린다. 례를 들어 ps지령이 수정되면 현재 체계에 존재하는 해커가 심어놓은 프로쎄스를 확인할 방법이 없습니다.

《붉은별》봉사기용체계 3.0을 설치할 때에 관리자만 알수 있는곳에 중요한 화일들을 별도로 압축보관했다가 이런 경우에 압축해제해서 수정된 화일을 교체하거나 체계상태파악을 보다 정확하게 할수 있습니다.

5. 체계디스크와 자료디스크구분에 의한 자료보안실현

《붉은별》봉사기용체계 3.0 설치할 때에 조작체계가 설치되는 체계공간과 사용자의 자료공간을 구분하여 각각 별도의 디스크나 또는 다른 구획에 설치합니다. 그래야 봉사기가 파괴되여 복구불가능한 상태일 때도 최소한의 사용자자료는 보존할수 있습니다.

6. 여벌복사를 다른 디스크에 진행하는 방법

《붉은별》봉사기용체계 3.0의 여벌복사공간(실례: /backup)은 가능하면 별도의 디스크를 리용합니다. 물론 이 경우에도 국부여벌복사이기때문에완전히 믿을수는 없지만 일반 등록부에 그대로 여벌복사시키는것보다는 훨씬 효과적입니다.

7. root의 crontab 국부여벌복사설정으로 자료대피

봉사기의 여벌복사를 국부에서 하는가, 원격에서 하는가에 따라서 국부여벌복사와 원격여벌복사로 나눈다. 《붉은별》봉사기용체계 3.0을 설치한후에는 최소한 국부여벌복사는 수행되도록 설정해야 합니다. 대부분 국부여벌복사설정은 root의 crontab에 등록하고 주기적으로 여벌복사되도록 합니다. 따라서 봉사기설치후에 root의 crontab에 국부여벌복사가 수행되도록 다음과 같이 등록합니다. 다음은 국부여벌복사수행을 위하여 root 권한으로 “crontab -e”를 실행하여 crontab에 등록한 내용입니다.

```
10 04 * * * /root/backup.sh >& /dev/null
```

이 지령은 매일 4시 10분에 /root/backup.sh 프로그람을 실행한다는 의미입니다. 그러면 /root/backup.sh 쉘스크립트화일에 어떤 지령이 있는가를 보자

```
#crontab –e
#!/bin/bash
#This is backup shell program

mount /dev/sda6 /backup
rsync –avz localhost:/var/lib/mysql/ /backup
umount /backup
```

여기서 주의할것은 backup.sh화일을 창조할 때 화일허가가 기정적으로 설정된 값인 644로 되는데 이것을 544로 해주어야 합니다.

여기서 mount지령은 여벌복사디스크의 보안을 위해 여벌복사시에만 탑재합니다. 대부분의 여벌복사작업을 할 때에는 먼저 여벌복사 쉘스크립트를 cron에 넣어두고 자동여벌복사되도록 합니다. 이때 이 쉘스크립트안에서 여벌복사하기전에 mount를 수행하고 여벌복사하도록 하고 여벌복사한후에는 다시 umonut를 해서 탑재해제하도록 합니다.

이렇게 하면 불가피하게 해킹을 당하여 “rm –rf /”가 수행되더라도 최소한 여벌복사디스크의 내용만은 삭제되지 않습니다. 즉 여벌복사자료가 보관되는 여벌복사디스크의 화일체계를 여벌복사할 때에만 탑재하고 평상시에는 탑재해제되도록 하는 방법입니다.

8. /etc/xinetd.d/의 불필요한 봉사화일의 뒤문없애기

봉사기를 설치한후에 /etc/xinetd.d 등록부에서 불필요한 xinetd 봉사화일들을 모두 삭제해야 합니다. 실례로 finger 와 같은 화일이 존재한다면 외부에서 이 봉사기의 접속자정보를 확인할수 있습니다.

9. /etc/rc.d/init.d/불필요한 초기화화일들을 삭제

설치직후에 /etc/rc.d/init.d/등록부에서 필요하지 않은 봉사스크립트화일들을 모두 삭제해야 합니다. 이 등록부에는 체계가 기동되면서 자동실행할 봉사스크립트화일들이 들어있습니다. 례를 들어 /etc/rc.d/init.d/nfs 또는 /etc/rc.d/init.d/smb 등과 같이 스크립트가 존재할경우에는 nfs 의 사용으로 화일체계가 원격탑재가 가능하게 되고 samba 를 리용하여 원격화일공유가 가능하게 됩니다.

10. /etc/services 에서 사용하지 않는 포구정보설명처리

/etc/services 화일은 체계에서 사용하는 봉사포구정보를 정의하고 있는 화일입니다. 관리자들이 착각하기 쉬운것은 이 화일에서 특정봉사가 정의되여 있다고 해서 그 포구가 열려있다는 의미는 아닙니다. 특정포구가 열려있다는 의미는 그 포구번호를 사용하는 특정한 봉사프로쎄스가 실행되고 있다는 의미입니다. 따라서 /etc/services 화일에서 정의된 모든 봉사들이 열려있다는 의미는 결코 아닙니다.

그러나 가능하면 /etc/services 화일에 정의된 봉사들중 사용하지 않는 봉사들은 삭제해야 합니다.

11. /etc/hosts.allow, /etc/hosts.deny 화일에서 접근허용설정

《붉은별》봉사기용체계 3.0 에서 봉사기접근조종을 하는 가장 기본적인 tcp_wrapper 의 설정화일이 /etc/hosts.allow 화일과 /etc/hosts.deny 화일입니다. 이 화일에 관리자나 특정사용자만이 접근조종할수 있도록 설정해야 합니다.

12. 규정위반사용자식별자특별관리

봉사기를 관리해보면 봉사기가입규정을 제대로 지키지 못해서 부득히 규정위반사용자가입을 일시 중시해야 하는 경우가 있습니다. 여기서는 이런 경우 어떻게 처리해야 하는가에 대한 방법들을 설명합니다.

가입자가 봉사기가입규정을 한 두가지 지키지 못했다고 하여 사용자식별자를 삭제할 필요는 없습니다.

그러나 봉사기가입을 못하게 하면서도 홈페지는 정상적으로 돌아가도록해야 합니다. 그리고 자기결함을 시정했을 경우에는 이전에 사용하던 사용자식별자를 그대로 사용하여 다시 가입을 할수 있도록 해야 합니다.

이런 경우 먼저 passwd 지령으로 해당 사용자 jbc 의 통과암호에 lock 를 걸어둡니다.

```
[root@c5 etc]# passwd -l jbc
jbc 사용자의 암호 잠금
passwd: 성공
[root@c5 etc]#
```

이 지령이 실행되기전 /etc/shadow 화일의 맨 마지막행은 다음과 같습니다.

```
xfs:!!:15843:0:99999:7:::
pegasus:!!:15843:0:99999:7:::
gdm:!!:15843:0:99999:7:::
jbc:$1$Sv3vGWMy$JvR3dI6qK3nMMrjGAec6h/:15843:0:99999:7:::
```

이 지령을 실행한 후의/etc/shadow 화일의 맨 마지막행은 다음과 같습니다.

```
xfs:!!:15843:0:99999:7:::
pegasus:!!:15843:0:99999:7:::
gdm:!!:15843:0:99999:7:::
jbc:!!$1$Sv3vGWMy$JvR3dI6qK3nMMrjGAec6h/:15843:0:99999:7:::
```

/etc/shadow 화일을 보면 통과암호문자렬앞에 “!!”문자가 추가된것을 확인할수 있습니다. 이렇게 lock 를 걸면 어떤 통과암호도 인증되지 않기때문에 jbc 사용자는 봉사기에 가입할수 없습니다. 물론 telnet, ftp 에도 가입할수 없습니다.

그러나 봉사기접속외의 모든것은 정상적으로 동작합니다. 즉 jbc 사용자의 홈페지와 MYSQL 자료기지등 모든것이 정상이지만 단지 봉사기접속만을 할수없게 됩니다. 사용자가 자기결함을 시정했을경우에는 다시 원상대로 되돌려야 합니다.

이때에는 다음과 같이 지령을 실행시킵니다.

```
[root@c5 etc]# passwd -u jbc
jbc 사용자의 암호 잠금해제중
passwd: 성공
[root@c5 etc]#
```

간단한 방법이지만 매우 효과적인 가입자처리방법입니다. 만약 오래동안 lock처리를 해두었음에도 불구하고 계속 결함이 나타날때에는 다음대책으로 apache의 httpd.conf에 설정되여 있던 jbc사용자의 가상주콤퓨터설정을 설명처리하여 홈페지까지 펼쳐지지 않도록 합니다. 홈페지까지 중지하였음에도 계속 결함이 있을때에는 userdel지령으로 해당가입자의 자료를 모두 삭제처리할수 있습니다. 그러나 만약의 경우를 위하여 가능한 여벌복사는 해두어야 합니다.

13. root 권한으로 체계에 가입하는것은 보안상위법행위

봉사기관리자들은 체계에 가입할 때 대체로 원격에서 root권한을 가지고 가입합니다. 이때에 통과암호를 해킹당하는 실례가 많습니다. 따라서 관리자들은 일반사용자로 가입해서 작업을 해야 하며 반드시 root권한으로 작업할필요가 있을때는 su지령을 리용해서 root권한을 획득하여 작업을 해야 합니다.

su지령으로 root권한을 획득하는 방법은 다음과 같습니다.

```
login as: jbc
jbc@172.29.88.105's password:
Last login: Sat May 25 16:15:40 2013 from 172.29.88.91
[jbc@c5 ~]$ su
암호:
[root@c5 jbc]#
```

현재 jbc일반사용자식별자로 가입하였다는것을 알수있습니다. 다음 su지령을 입력하고 실행하면 password입력대기상태로 이행하며 이때 root통과암호를 입력하면 root사용자식별자로 합니다. 이를 확인하기 위해 ls –l지령을 실행합니다. 결과는 root사용자식별자의 홈등록부의 내용이 현시됩니다. 결국 root권한을 획득하였다는것을 알수 있습니다.

14. 같은 종류의 프로쎄스 한번에 모두 끄기

봉사기관리를 하다보면 특정한 프로쎄스가 체계자원을 너무 많이 사용하여 속도가 떠지거나 일시적인 고장이 발생하는 경우가 있으며 또한 흔히 보지 못했던 비정상적인 프로쎄스를 발견하였을 때에 대부분 ps로 해당 프로쎄스의 PID를 확인한 다음 "kill -9 PID"와 같은 방법으로 특정한 프로쎄스를 정지시켜 응급대책를 합니다.

만약 삭제해야 할 프로쎄스가 한개가 아니라 열개 이상이라면 kill지령을 모두 10번 사용해야 합니다. 여기서 설명하는 방법은 동일한 이름을 가진 여러개의 프로세스를 한번에 삭제할 경우에 매우 편리한 방법입니다.

일반적으로 특정 프로쎄스를 확인하는 방법은 ps라는 지령을 리용하여 다음과 같이 할수 있습니다.

```
[root@c5 jbc]# ps -ef | grep sshd
root       1186     1  0 07:39 ?        00:00:00 /usr/sbin/sshd
root       2892  1186  0 08:58 ?        00:00:00 sshd: root@pts/5
root       3697  1186  0 10:11 ?        00:00:00 sshd: kim [priv]
kim        3701  3697  0 10:11 ?        00:00:00 sshd: kim@pts/0
root       5917  1186  0 12:00 ?        00:00:00 sshd: root@notty
root       7910  1186  0 15:07 ?        00:00:00 sshd: root@pts/1
root       8572  1186  0 15:53 ?        00:00:00 sshd: root@pts/7
root       9402  1186  0 16:21 ?        00:00:00 sshd: jbc [priv]
jbc        9406  9402  0 16:21 ?        00:00:00 sshd: jbc@pts/4
root       9565  9441  0 16:27 pts/4    00:00:00 grep sshd
[root@c5 jbc]# kill -9 3697
[root@c5 jbc]# ps -ef | grep sshd
root       1186     1  0 07:39 ?        00:00:00 /usr/sbin/sshd
root       2892  1186  0 08:58 ?        00:00:00 sshd: root@pts/5
kim        3701     1  0 10:11 ?        00:00:00 sshd: kim@pts/0
root       5917  1186  0 12:00 ?        00:00:00 sshd: root@notty
root       7910  1186  0 15:07 ?        00:00:00 sshd: root@pts/1
root       8572  1186  0 15:53 ?        00:00:00 sshd: root@pts/7
root       9402  1186  0 16:21 ?        00:00:00 sshd: jbc [priv]
jbc        9406  9402  0 16:21 ?        00:00:00 sshd: jbc@pts/4
root       9580  9441  0 16:28 pts/4    00:00:00 grep sshd
[root@c5 jbc]#
```

```
[root@c5 jbc]# killall sshd
[root@c5 jbc]# ps -ef | grep sshd
```

15. ping 에 응답하지 않게 설정하는 보안

ping 은 봉사기나 망에서 관리자들과 사용자들이 필수적으로 사용하는 통신검사지령입니다.

그러나 이런 ping 지령이 다른 목적으로 사용되는 경우가 있습니다. 례를 들어 특정봉사기에 부하를 주기 위하여 파케트크기를 조절하여 ping 검사를 시도한다든가 지속적인 ping 검사로 봉사기나 망의 부하를 일으킨다든가 특정봉사기의 해킹을 목적으로 봉사기가 운영중인가를 확인하기 위해 사용하는 경우등이 있습니다. 이런 경우 보안을 위하여 ping 에 응답하지 않게 설정할 수 있습니다.

다음과 같이 설정함으로서 ping 검사에 대한 응답을 못하게 하거나 다시 응답할수 있습니다.

그 방법은 /proc/sys/net/ipv4/icmp_echo_ignore_all 화일값을 1 로 설정합니다.

다시 응답하게 하려면 /proc/sys/net/ipv4/icmp_echo_ignore_all 화일값을 0 으로 설정합니다.

```
[root@c5 jbc]# cd /proc/sys/net/ipv4
[root@c5 ipv4]# pwd
/proc/sys/net/ipv4
[root@c5 ipv4]# echo 1 > icmp_echo_ignore_all
[root@c5 ipv4]# echo 0 > icmp_echo_ignore_all
[root@c5 ipv4]#
```

16. Root 소유의 SetUID, SetGID 화일 조사

《붉은별》봉사기용체계 3.0 에는 root 소유로 되여있는 SetUID 화일들과 SetGID 화일들이 수없이 존재합니다. 이런 화일들중에서 거의 대부분은 SetUID 가 설정되여있지 않아도 되는 화일들입니다. 만약 특정화일에 SetUID 가 설정되여 있다면 그 화일이 실행되는 동안은 root 권한을 사용하게 됨으로 반드시 필요하지 않는 화일(지령)들은 SetUID, SetGID 를 제거하는것이 좋습니다. 먼저 체계 전체에서 root 소유의 SetUID 화일을 검색한 실례를 봅시다.

```
[root@c5 ipv4]# find / -user root -perm -4000 -print
/usr/sbin/userhelper
/usr/sbin/usernetctl
/usr/sbin/suexec
/usr/libexec/openssh/ssh-keysign
/usr/libexec/pt_chown
/usr/libexec/polkit-1/polkit-agent-helper-1
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/crontab
/usr/bin/su
/usr/bin/rlogin
/usr/bin/passwd
/usr/bin/ksu
/usr/bin/chsh
/usr/bin/rcp
/usr/bin/pkexec
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/rsh
/usr/bin/newrole
/usr/bin/chage
/sbin/pam_timestamp_check
/sbin/unix_chkpwd
/sbin/mount.nfs
find: `/proc/9931/task/9931/fd/5' 그런 화일이나 등록부가 없습니다.
find: `/proc/9931/task/9931/fdinfo/5' 그런 화일이나 등록부가 없습니
다.
find: `/proc/9931/fd/5' 그런 화일이나 등록부가 없습니다.
find: `/proc/9931/fdinfo/5' 그런 화일이나 등록부가 없습니다.
/lib/dbus-1/dbus-daemon-launch-helper
/bin/fusermount
/bin/ping
/bin/mount
/bin/umount
/bin/ping6
[root@c5 ipv4]# ^C
```

여기서 ping지령은 SetUID가 설정될 리유가 전혀 없습니다. 이 지령은 거의 root만 사용할뿐 일반사용자들은 잘 사용하지 않습니다. 따라서 이 지령은 권한을 다음과 같이 설정합니다.

```
[root@dell-rss home]# ls -l /bin/ping
-rwsr-xr-x  1 root root 35108  2004  6월 16 09:13 /bin/ping
[root@dell-rss home]# chmod 100 /bin/ping
[root@dell-rss home]# ls -l /bin/ping
---x------  1 root root 35108  2004  6월 16 09:13 /bin/ping
[root@dell-rss home]#
```

원래 이 지령의 기본 권한은 4755 였습니다. 이를 100 으로 설정하였습니다. 즉 SetUID 를 제거하고 오직 root 만 사용할수 있게 설정하였습니다. 이와 같이 SetUID 를 제거하고 일반사용자들은 사용할수없게 최소한의 권한만을 설정해야 합니다.

17. su 지령사용만을 확인하는 방법

봉사기에 등록가입한 흔적을 조사해야 하는 경우에 가장 우선적으로 확인해야 할 사항이 있습니다. 즉 su 라는 지령을 리용하여 root 권한을 언제, 누가 획득하여 사용하였는가에 대한 리력입니다. 대부분의 봉사기에서는 root 사용자식별자로 직접 가입하지 않으므로 일반사용자식별자로 등록가입한 후에 su 지령을 사용하여 root 권한을 획득하게 됩니다. 대부분 정당한 권한이 있는 관리자에 의한 root 권한획득이겠지만 이따금 해킹당한 봉사기에서 볼수 있는 su 지령을 리용한 불법적인 root 권한획득흔적이 있기때문입니다. 그러므로 반드시 su 지령사용리력을 확인해야 합니다.

아래의 실례는 “grep “su:” /var/log/secure”를 실행한 실례입니다.

```
[root@localhost log]# grep "su:" /var/log/secure
May 25 17:59:47 localhost su: pam_unix(su:session): session opened for user root by jbc(uid=500)
[root@localhost log]#
```

/var/log/secure 화일에는 주로 사용자들의 원격등록가입정보를 기록하고 있는 기록화일로서 봉사기보안에 아주 민감한 중요한 화일입니다. 특히 tcp_wrapper(xinetd)의 접속조종에 대한 기록화일로서 언제 누가 어디에서 어떻게 접속을 했는가에 대한 기록을을 기록을하고 있습니다.

체계의 불법침입등이 있었다고 의심될때는 반드시 이 기록화일을 확인해야 합니다. 따라서 우의 지령은 grep 라는 지령을 리용하여 /var/log/secure 화일에 보관되여있는 내용들 가운데서 “su:”라는 문자렬이 있는 행만을 확인한 것입니다.

우의 결과를 보면 5 월 25 일 17 시 59 분 47 초에 jbc 라는 사용자가 su 지령을 리용하여 root 권한을 획득하였다는것을 확인할수 있습니다.

/var/log/secure 라는 기록화일은 /etc/rsyslog.conf 화일에 정의되여 있습니다. /var/log/secure 화일은 체계의 인증과 데몬들의 사건발생에 대한 내용을 모두 기록하고 있는 화일입니다.

/etc/rsyslog.conf 화일에는 secure 화일의 위치를 변경할수도 있으므로 앞으로 /etc/rsyslog.conf 화일에서 secure 화일의 위치를 정확히 확인해보기 바란다. 중요한 기록화일은 다른 위치에 보관하도록 설정할것을 권고합니다.

18. 기본실행되는 불필요한 프로쎄스제거

《붉은별》봉사기용체계 3.0 에는 많은 프로쎄스들이 실행되고 있지만 이 모든것이 사용되는것은 결코 아닙니다. 따라서 이런 프로쎄스들을 실행상태로 그대로 두면 체계자원을 랑비하게 되고 외부의 불법적인 침입에 리용되게 됩니다. 그러므로 필요없는 프로쎄스들은 제거하여야 합니다.

현재 체계에서 실행되고 있는 프로쎄스들을 확인하는 방법은 ps 나 pstree, top 지령들을 리용할수 있습니다. 이 지령들을 리용하면 실행되고 있는 프로쎄스의 PID 를 확인할수 있고 해당 프로쎄스를 제거하려면 "kill –9 PID"를 실행하면 됩니다. 그러나 재기동하면 다시 실행됩니다.

《붉은별》봉사기용체계 3.0 에서 프로쎄스가 실행되는것은 다음과 같은 경우입니다.

- 사용자에 의한 지령실행.
- 핵심부에 의한 체계관리프로쎄스
- /etc/rc.d/init.d/* 스크립트화일에 의한 프로쎄스실행.
- /etc/xinetd.d/* 화일들의 실행 (xinetd 대몬이 실행함.)
- 기타.

이과 같이 프로쎄스가 실행되는 경우가 많기 때문에 간단히 나누어서 설명합니다.

이미 앞부분에서/etc/rc.d/init.d/등록부에서 불필요한 스크립트화일삭제는 이미 설명하였고 /etc/xinetd.d/등록부에서 xinetd 환경에서 봉사되는 불필요한 봉사화일들은 삭제하는 설명도 이미 취급되였습니다. 때문에 여기서는 체계기동과 함께 실행되로록 하는 ntsysv 도구에 대하여서만 설명합니다.

《붉은별》봉사기용체계 3.0 에서 ntsysv 를 실행하면 다음과 같은 창문이 열립니다.

이 화면의 매 항목들은 사실 /etc/rc.d/init.d/등록부들과 /etc/xinetd.d/등록부들에 있는 봉사화일들의 이름을 현시한것입니다.

이것은 조작탁에서 실행시킨 결과이며 만약 원격에서 실행시켰어도 결과화면은 같습니다. 이 화면을 보면서 기동시에 기동시키지 않으려는 봉사대몬들은 “*”를 제거하면 됩니다.

19. /etc/rc.d/rc.local 화일에 기동시에 기동할 화일등록

/etc/rc.d/rc.local 화일은 봉사기기동단계의 맨 마지막단계에서 실행되는 화일입니다. 따라서 봉사기기동시마다 자동기동하려고 하는 경우에는 이 화일에 등록을 합니다.

대부분 자체로 만든 응용프로그람의 자동실행을 위한것입니다.

```
[root@localhost ~]# cat /etc/rc.d/rc.local
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
[root@localhost ~]#
```

20. 화일과 디스크보안을 위한 방법들

일반적으로 보안이라고 하면 방화벽이나 IDS 와 같은 보안장비를 생각하게 됩니다. 그러나 이외에도 간단한 방법으로 큰 효과를 얻을수 있는 화일과 디스크보안방법이 있습니다.

1) 체계화일과 원본을 한부 복사하여 숨기기.

체계와 관련된 중요한 지령이나 설치화일들은 특별한 등록부를 만들어서 보관합니다. 실례로 봉사기가 해킹당하여 ps 나 find 지령이 변화되였다면 변화된 화일을 삭제하고 원래의 상태를 회복해야 합니다. 숨길 등록부이름은 .(점)으로 시작하는 이름을 사용하는것이 좋습니다. 실례에서는 /backup/.hidden/.files/라는 위치에 등록부를 만들어서 보관하고 있습니다. 이 화일들은 ls –l 지령에서는 보이지 않습니다.

2) chattr 지령으로 화일이 변경되지 않도록 설정.

대부분 해킹도구들이 실행되면 중요한 지령이나 화일들은 변화됩니다. 하지만 화일에 i 속성이 들어있다면 해킹도구에 의해 변화되지 못합니다. 따라서 해킹할 가능성이 줄어들게 됩니다. 실례로 /bin/ps 화일을 대상으로 "chattr+i /bin/ps"를 실행시키면 /bin/ps 화일은 삭제, 추가 변갱이 전혀 되지 않습니다. 이를 위해 먼저 lsattr 로 /bin/ps 화일에 부여되여 있는 화일의 속성을 확인합니다.

```
[root@dell4-jbc bin]# lsattr /bin/ps
------------- /bin/ps
[root@dell4-jbc bin]# █
```

즉 아무런 속성도 부여되여 있지 않습니다.

```
[root@www home]# chattr +i /bin/ps
[root@www home]# lsattr /bin/ps
----i-------- /bin/ps
[root@www home]# █
```

다시 보면 i 속성이 부여되여 있다는것을 확인할수 있습니다. 다음은 /bin/ps 를 root 권한으로 삭제해보면 절대로 삭제되지 않습니다.

3) 화일체계읽기전용으로 탑재

일반적으로 ftp 봉사들은 읽기전용으로 탑재합니다.

mount 지령사용시에 –r 선택항목을 사용하면 읽기전용으로 탑재할수 있습니다. 일반적으로 선택항목이 없이 그대로 탑재하면 기본값으로 읽기/쓰기방식으로 탑재합니다. 그리고 /etc/fstab 화일의 탑재선택항목에서 ro 선택항목을 사용하면 매번 기동할 때마다 탑재시에 지속적으로 읽기전용방식으로 탑재할수 있습니다. 아래 실례는 /etc/fstab 화일에서 /downloads 라는 탑재점으로 탑재하면서 읽기전용으로 탑재한것입니다.

#mount –t ext3 –r /dev/sda2 /downloads

다음은 mount 지령을 실행하여 현재의 탑재정보를 확인한것입니다. 결과의 맨 마지막행을 보면 /dev/sda2 가 /downloads 등록부에 읽기방식으로 탑재된 것을 알수 있습니다.

mount

이와 같이 탑재를 하면 /downloads 에는 어떤 화일도 삭제되지 않을뿐아니라 변경되지도 않습니다. 물론 새로운 화일도 보관되지 않습니다.

다음은 기동시에 자동탑재설정화일인 /dtc/fstab 화일에서 /downloads 라는 탑재점에 ro 라는선택항목을 사용하여 매번 읽기전용으로 탑재되도록한것입니다.

```
[root@localhost ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Sat May 25 10:05:42 2013
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=be1c3757-0499-4dad-a6a2-a746698e7a1c /                       ext3    defaults
/dev/sda6               swap                    swap    defaults        0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/sda2               /downloads              ext3    ro              1 2
[root@localhost ~]#
```

21. SetUID, SetGID, StickyBit 설정

SetUID, SetGID, StickyBit 에 대하여 실례를 들어 설명합니다. Passwd 지령은 /usr/bin/passwd 의 화일형태로 존재합니다. 그리고 일반사용자들은 이 지령을 실행하여 /etc/passwd 또는 /etc/shadow 화일에 보관되여 있는 자기의 통과암호를 수정합니다. 물론 이 지령은 사용자식별자를 가진 사용자라면 누구나 다 실행할수 있습니다.

다음은 3 개의 화일에 대한 권한을 확인해봅니다.

```
[root@dell-rss home]# ls -l /usr/bin/passwd
-r-s--x--x  1 root root 19336  2004  9월  7 17:11 /usr/bin/passw
[root@dell-rss home]# ls -l /etc/passwd
-rw-r--r--  1 root root 2520  2009  5월 28 16:35 /etc/passwd
[root@dell-rss home]# ls -l /etc/shadow
-r--------  1 root root 1536  2009  5월 28 16:35 /etc/shadow
[root@dell-rss home]#
```

실례에서 알수 있는 바와 같이 /etc/passwd 화일과 /etc/shadow 화일의 권한은 각각 644 와 400 입니다. 즉 root 사용자외에 일반사용자는 변경할수 없습니다.
그러나 사용자식별자를 가진 사용자라면 누구나 이 화일에 대한 자신의 통과암호를 변경할수 있습니다. 이런 불일치의 원인은 바로 SetUID 에 있습니다.
우에서 보는바와 같이 /usr/bin/passwd 화일은 root 소유이고 SetUID 가 설정되여 있습니다. 따라서 일반사용자들이 /usr/bin/passwd 지령을 실행하여 /etc/passwd 화일에 있는 자신의 통과암호를 변경하려고 할 때 실행시킨 일반사용자의 권한으로 실행되는것이 아니라/usr/bin/passwd 지령의 소유자인 root 권한으로 실행됩니다.
일반사용자들도 /usr/bin/passwd 지령을 리용하여 /etc/passwd 화일과 /etc/shadow 화일을 수정하여 자신의 통과암호를 수정할수 있습니다. 즉 특정화일이나 지령에 SetUID 가 설정되여 있다면 그 화일(지령)을 실행시킬때에는 실행시킨 사용자의 권한으로 실행되는것이 아니라 그 화일(지령)의 소유자의 권한으로 실행됩니다. 이것이 바로 SetUID 의 의미이며 효과입니다. 그리고 SetUID, SetGID 와 Stickybit 는 일반 권한외에 다른 방법으로 그 설정을 표시하고 있습니다.

4XXX : SetUID 를 의미합니다. (XXX 는 일반권한)

2XXX : SetGID 를 의미합니다. (XXX 는 일반권한)

1XXX : Stickybit 을 의미합니다. (XXX 는 일반권한)

참고로 Stickybit 설정은 대부분 /tmp 등록부에 설정되여 있습니다. 목적은 공유등록부로 사용하기 위해서입니다. 즉 Stickybit 로 설정된 등록부는 모든 사용자가 쓰기가능하며 쓰기된 화일은 그 사용자의 소유로 생성됩니다. 물론 삭제할수 있는 권한은 root 소유자만이 가능합니다. 따라서 공동으로 사용할 등록부들에 Stickybit 를 설정하면 이런 수정들이 가능하게 됩니다.

- 특정화일에 SetUID bit 설정

특정화일에 이 비트가 설정되여 있다면 다른 사용자들이 그 화일을 실행하였을 경우에 실행되는 동안에는 실행시킨 사용자의 권한이 아닌 화일의 소유자권한으로 실행됩니다.

이 권한을 설정하는 방법은 4755, 4644, 4750 같이 지금까지 설명한 일반권한앞에 4를 붙이면 됩니다. 아래의 실례는 testfile 에 일반권한 755 와 함께 이 비트를 4로 설정한것입니다.

```
[root@dell-rss test]# ls -l
검사합 0
-rw-r--r--  1 root root 0  2009 10월 14 03:22 testfile
[root@dell-rss test]# chmod 4755 testfile
[root@dell-rss test]# ls -l
검사합 0
-rwsr-xr-x  1 root root 0  2009 10월 14 03:22 testfile
[root@dell-rss test]#
```

이 화일의 실행권한자리에 s 문자가 있으면 다른 사용자들이 이 화일을 실행하더라도 화일의 소유자권한으로 실행이 됩니다.

- 특정화일에 SetGID 설정.

앞에서와 같은 방법으로 하지만 4 대신에 2를 붙인다. 아래의 실례는 testfile 에 일반권한 755 와 함께 SetGID 비트를 2를 설정한것입니다.

```
[root@dell-rss test]# ls -l
검사합 0
-rw-r--r--  1 root root 0  2009 10월 14 03:31 testfile
[root@dell-rss test]# chmod 2755 testfile
[root@dell-rss test]# ls -l
검사합 0
-rwxr-sr-x  1 root root 0  2009 10월 14 03:31 testfile
[root@dell-rss test]#
```

이 화일의 그룹소유자권한자리에 s 문자가 있다는것은 SetGID 가 설정된 화일을 다른 사용자가 실행시키면 실행시킨 사용자의 권한으로 실행되는것이 아니라 화일의 소유자그룹권한으로 실행됩니다.

- 특정등록부에 Stickybit 설정.

《붉은별》봉사기용체계 3.0 에서 흔히 /tmp 등록부를 이 비트로 설정합니다. 이 등록부안에서 특정화일을 생성하면 생성한 사용자의 소유로 화일이 생성됩니다. 그리고 다른 사용자가 이 등록부안에서 다른 화일을 생성하면 그 사용자의 소유로 화일이 생성됩니다. 화일을 삭제할 때에도 생성한 사용자만이 그 화일을 삭제할수 있습니다. 이런 등록부를 공유등록부라고 합니다.

```
[root@dell-rss test]# ls -l
검사합 4
drwxr-xr-x  2 root root 4096  2009 10월 14 03:41 testdir
[root@dell-rss test]# chmod 1755 testdir
[root@dell-rss test]# ls -l
검사합 4
drwxr-xr-t  2 root root 4096  2009 10월 14 03:41 testdir
[root@dell-rss test]#
```

다른 사용자권한자리에 t 라는 문자가 설정된것을 볼수 있습니다. t 라는 문자의 의미는 Stickybit 라는것입니다.

만약 kim 이라는 사용자가 testdir 등록부에 kimfile 을 생성하였다면 kimfile 화일의 소유자는 kim 이 되고 삭제와 변경도 kim 만이 할수 있습니다. 그리고 pak 이라는 사용자가 이 등록부에 pakfile 을 생성하였다면 pakfile 화일의 소유자는 pak 이 되고 삭제와 변경도 pak 만이 할수 있습니다. 물론 root 사용자는 Stickybit 가 설정된 등록부에 대하여 얼마든지 삭제와 변경도 할수 있습니다.

- SetUID, SetGID, Stickybit 표시대소문자.

일부 SetUID, SetGID, Stickybit 설정표시가 소문자 s 가 아니라 대문자 S 로 표시된 경우가 있습니다. 이것은 다음과 같은 의미를 가진다.

대문자 S 로 표시된 SetUID 는 설정되여 있지만 일반권한에 실행권한이 존재하지 않음을 의미하며 따라서 SetUID 권한이 적용되지 않습니다.

대문자 S 로 표시된 Stickybit 는 설정되여 있지만 일반권한의 맨 마지막 자리에 실행권한이 존재하지 않음을 의미하며 따라서 Stickybit 권한이 적용되지 않습니다.

22. 원격봉사기의 사용자식별자정보확인

《붉은별》봉사기용체계 3.0 보안을 위하여 반드시 알아야 지령은 finger 지령입니다. 한마디로 finger 지령은 국부사용자 또는 원격사용자의 사용자식별자정보를 확인하는 지령입니다.

또한 finger 는 원격사용자가 국부사용자의 가입이름과 마지막가입시간과 같은 정보를 볼수있도록 하는 지령입니다. finger 지령은 지정된 사용자식별자의 정보를 /etc/passwd 화일에서 읽어서 보여줍니다. 확인할수 있는 정보로는 UID, 사용자명, 홈등록부위치, 기본사용자쉘, 현재 가입정보등입니다.

사용형식: finger [-lmsp] [사용자…] [사용자@주콤퓨터…]

또한 finger는 국부봉사기의 사용자뿐아니라 원격봉사기의 사용자정보까지 확인가능한 지령입니다. 따라서 봉사기관리자는 현재 관리하는 봉사기에서 finger봉사가 되지 않도록 설정하는것이 보안상 유리합니다. 즉 봉사기보안을 위하여/etc/xinetd.d/finger 화일을 삭제하고 /etc/services 화일안에 finger 행을 삭제하여 finger봉사를 끄는것이 봉사기사용자식별자정보를 보호하고 봉사기보안을 강화하는데서 중요합니다.

```
[root@localhost tftpboot]# finger jbc
Login: jbc                              Name: (null)
Directory: /home/jbc                    Shell: /bin/bash
Last login Wed Feb  6 14:38 2008 (KST) on :0
No mail.
No Plan.
[root@localhost tftpboot]#
```

-s 선택항목을 사용하면 우의 정보를 간단히 정리하여 볼수 있습니다.

```
[root@localhost tftpboot]# finger -s jbc
Login     Name       Tty      Idle  Login Time   Office     Office Phone
jbc                  :0          *  Feb  6  2008
[root@localhost tftpboot]#
```

봉사기관리자들은 finger봉사가 꼭 필요한것이 아니라면 다음 두가지 설정을 해서 봉사기보안을 강화해야 합니다.

첫째로: /etc/xinetd.d/finger 화일의 삭제.

둘째로: /etc/services 화일안에서 finger행의 삭제 또는 설명처리(#)를 해야합니다.

23. 봉사기부하률을 통한 보안점검

uptime은 체계의 부하률을 확인할수 있는 지령입니다. 즉 1분, 5분, 15분간격으로 체계의 평균부하률을 각각 출력합니다.

이 지령으로 알수 있는 정보들은 다음과 같습니다.

- 현재 시간.
- 체계가 기동한 후에 완료없이 얼마동안 운영하였는가?
- 현재 체계에 가입된 사용자수(/var/run/utmp 화일참조)
- 1분,5분,15분동안의 체계평균부하률.

이 지령은 봉사기관리자가 봉사기의 전체적인 부하률을 확인하려고 할 때 사용합니다. 또한 uptime은 top와 w의 실행결과에서 맨 첫번째행을 표시해

주는 역할을 합니다. 그리고 프로세스들의 정보를 확인하기 위하여 /proc 화일체계를 참조하기도 합니다.

```
[root@localhost work]# uptime
 20:34:35 up 1 day,  2:44,  2 users,  load average: 0.19, 0.33, 0.38
[root@localhost work]# █
```

결과의 의미는 다음과 같습니다.

- 20:34:35 : 현재 시간이 20시 34분 35초.
- up 1 day : 1일동안 재기동되지 않고 계속 운영되였음.
- 2:44 : 2시간 44분동안 기동되여 있습니다.
- 2 users : 체계에 가입한 사용자수 2명.
- load average : 0.19, 0.33, 0.38 : 각각 1분, 5분, 15분동안의 체계평균부하률.

여기서 중요한것은 체계부하률입니다. 이 정보를 가지고 체계 정확한 상태를 파악하기 힘들지만 체계부하가 있었는가는 확인할수 있습니다. 이 3개의 수자가 지내 크면 많은 해킹프로쎄스들의 실행으로 CPU나 Memory에 부하가 있다고 판단하고 즉시 대책을 세워야 합니다.

24. 보안을 위한 find 활용

여기서는 일반적인 find지령의 화일검색은 제외하고 보안과 관련된 find의 특수기능에 대하여 설명합니다.

► root 소유의 SetUID화일탐색.

체계에 존재하는 화일들가운데서 root 소유의 SetUID화일은 매우 제한적인 용도로만 사용합니다. root 소유의 SetUID화일은 실행시에 root권한으로 실행됨으로 반드시 관리해야할 화일들입니다. 따라서 봉사기관리자는 주기적으로 root 소유의 SetUID화일을 검색해 보아야 합니다.

```
[root@localhost ~]# find / -user root -perm -4000 -print
/bin/mount
/bin/ping
/bin/ping6
/bin/umount
/bin/su
/bin/fusermount
/sbin/pam_timestamp_check
/sbin/mount.nfs
/sbin/unix_chkpwd
find: `/proc/2542/task/2542/fd/5' 그런 화일이나 등록부가 없습니다.
find: `/proc/2542/task/2542/fdinfo/5' 그런 화일이나 등록부가 없습니다
find: `/proc/2542/fd/5' 그런 화일이나 등록부가 없습니다.
find: `/proc/2542/fdinfo/5' 그런 화일이나 등록부가 없습니다.
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/chage
/usr/bin/rlogin
/usr/bin/newrole
/usr/bin/rsh
/usr/bin/newgrp
/usr/bin/crontab
/usr/bin/chsh
/usr/bin/rcp
/usr/bin/at
/usr/bin/gpasswd
/usr/bin/ksu
/usr/bin/su
/usr/sbin/userhelper
/usr/sbin/suexec
/usr/sbin/usernetctl
/usr/libexec/polkit-1/polkit-agent-helper-1
/usr/libexec/openssh/ssh-keysign
/usr/libexec/pt_chown
/lib/dbus-1/dbus-daemon-launch-helper
[root@localhost ~]#
```

이렇게 탐색된 root 소유의 SetUID 화일들을 모두 하나씩 그 용도와 목적을 확인한후 불필요한것들은 삭제해야 합니다. 또한 아래와 같이 root 소유의 SetUID 화일을 찾을수 있습니다.

```
[root@dell-rss ~]# find / type f \( -perm -004000 -o -perm -002000 \) -exec ls -lg {} \;
-rwsr-xr-x  1 root 23332  2004 10월 11 16:57 /bin/traceroute
-rwsr-xr-x  1 root 80072  2008  5월 16 17:50 /bin/mount
-rwsr-xr-x  1 root 50188  2008  5월 16 17:50 /bin/umount
-rwsr-xr-x  1 root 12408  2004  6월 16 09:13 /bin/traceroute6
-rwsr-xr-x  1 root 30948  2004  6월 16 09:13 /bin/ping6
-r-s--x--x  1 root 16930  2004 11월 30 21:36 /sbin/pam_timestamp_check
-r-sr-xr-x  1 root 40964  2004 11월 30 21:36 /sbin/unix_chkpwd
-r-sr-xr-x  1 root 251554  2004 11월 30 21:36 /sbin/pwdb_chkpwd
-rwxr-sr-x  1 root 10843  2008  8월 19 08:21 /sbin/netreport
```

앞의 실례는 root 소유의 SetUID 만을 찾는다면 이 실례는 SetGID 까지 모두 찾는 실례입니다.

- 봉사기에서 뒤문화일탐색

봉사기에서 뒤문화일이 생성되는 위치는 대부분 /dev 입니다. /dev 에는 일반적으로 장치화일들만 존재하며 일반화일은 존재하지 않습니다. 따라서 /dev 등록부에서 일반화일을 검색하여 만약 존재한다면 거의 대부분은 뒤문으로 사용되고 있는 화일이라고 볼수 있습니다.

아래의 실례는 /dev 에 존재하는 화일들중 일반화일(-type f)을 찾아서 확인한것입니다.

```
[root@dell-rss ~]# find /dev -type f -exec ls -l {} \;
-rw-r--r--  1 root root 212992  2009 10월 20 14:14 /dev/.udev.tdb
[root@dell-rss ~]# █
```

이 화일외에 실지는 46 개의 화일이 존재합니다. 이 46 개화일외에 추가적인 화일이 발견된다면 반드시 뒤문화일로 판단해야 합니다.

- 봉사기내부의 .rhosts 화일을 검색.

《붉은별》봉사기용체계 3.0 에서 .rhosts 화일은 외부에서 아무런 제한없이 등록가입할수 있는 접근허용이 설정된 화일입니다. 이 화일이 존재한다면 반드시 확인해야 합니다. 아래 실례는 체계전체(/)를 대상하여 .rhosts 화일이 존재하는가를 보여달라(ls -l {})는 의미입니다.

```
[root@dell-rss dev]# find / -name .rhosts -exec ls -l {} \;
[root@dell-rss dev]# █
```

- 봉사기내부에서 .bash_history 화일을 모두 찾아서 확인.

.bash_history 화일은 root 를 포함하여 매 사용자들의 홈등록부에 존재하는 화일로서 매 사용자들이 사용하였던 지령이 보관되여 있는 매우 중요한 화일입니다. 만약 이 화일중 화일용량이 0 인 화일이 있다면 해킹가능성을 의심해야 합니다.

특히 root 소유자의.bash_history 화일용량이 0 이라면 이것은 매우 심각한 경우로서 거의 90%이상은 해킹되였다고 확신할수 있습니다.

```
[root@localhost ~]# find / -name .bash_history -exec ls -l {} \;
-rw-------. 1 root root 400  5월 26 10:13 /root/.bash_history
-rw-------. 1 kim kim 162  5월 26 10:28 /home/kim/.bash_history
[root@localhost ~]#
```

- 소유자 또는 소유그룹이 없는 화일탐색

《붉은별》봉사기용체계 3.0 는 많은 사람들이 함께 사용하는 다중사용자조작체계입니다. 따라서 모든 화일들과 등록부들은 소유자와 소유그룹을 가지고 있습니다. 그러나 간혹 이런 화일들이 존재하는 경우를 볼수 있습니다. 이런 화일들은 봉사기관리와 보안에 중요하게 관계되는 화일들입니다.

```
[root@dell-rss dev]# find / -nouser -o -nogroup -print
find: /proc/23462/task/23462/fd/4: 그런 화일이나 등록부가 없습니다.
find: /proc/23462/task/23462/fd/4: 그런 화일이나 등록부가 없습니다.
find: /proc/25290: 그런 화일이나 등록부가 없습니다.
find: /proc/25291: 그런 화일이나 등록부가 없습니다.
[root@dell-rss dev]#
```

지금까지의 실례와 다른점은 이 실례에서는 론리연산이 들어간다는것입니다. 우의 실례에서 –o 는 "OR"이라는 론리연산자를 의미합니다. –nouser 와 –nogroup 는 소유자, 소유그룹이 존재하지 않는 두가지중 어느 하나에 해당하는 경우에 화일탐색입니다.

- 관리자지령과 일반지령경로탐색.

앞에서 설명하였지만 《붉은별》봉사기용체계 3.0 는 많은 사용자들이 함께 사용하는 다중사용자조작체계입니다. 따라서 봉사기의 사용자는 관리자와 일반사용자로 구분되여 있습니다. 즉 관리자가 사용하는 지령과 일반사용자가 사용하는 지령은 차이난다.

일반사용자들이 사용하는 지령은 관리자가 모두 사용할수 있지만 일반사용자는 관리자가 사용하는 지령가운데서 일부는 일반사용자가 사용하지 못하도록 설정되여 있습니다. 이 구분을 위하여 《붉은별》봉사기용체계 3.0 에서는 지령탐색경로인 PATH 라는것을 설정하고 있습니다. 즉 어떤 사용자가 어떤 지령을 실행했을경우에 실행한 지령을 어디에서 부터 찾아서 실행할것인가라는것이 지령 PATH 를 의미합니다.

따라서 실행하려고 하는 지령을 찾는경로에 있어서 관리자경로와 일반사용자의 경로가 다르다는것을 의미합니다. 즉 봉사기를 관리하는 관리자의

립장으로부터 봉사기보안을 위하여 관리자 PATH 와 일반사용자 PATH 를 구분하여 관리해야 한다는 결론을 얻을수 있습니다.

다음은 root 사용자의 지령탐색경로를 확인한것입니다. 《붉은별》봉사기용체계 3.0 의 많은 쉘변수들가운데서 PATH 라는 변수가 바로 지령의 탐색경로를 보관하고 있는 변수입니다.

```
[root@localhost /]# id
uid=0(root) gid=0(root) 집단=0(root) 문맥=root:secadm_r:secadm_t:s0-s15:c0.c1023
[root@localhost /]# echo $PATH
/usr/kerberos/sbin:/usr/kerberos/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/bin:/b
in:/root/bin
[root@localhost /]#
```

우의 결과는 root 사용자가 특정지령를 실행하였을때에 어떤장소에서 그 지령을 찾을것인가를 확인한것입니다. 먼저 id 라는 지령으로 root 사용자임을 확인합니다. 그다음 "echo $PATH"를 실행하여 root 사용자의 PATH 를 확인합니다. 즉 root 관리자가 어떤 지령을 실행하였을때 그 지령을 찾는 순서는

/usr/kerberos/sbin

/usr/kerberos/bin

/usr/local/sbin

/usr/local/bin

/sbin

/bin

/usr/sbin

/usr/bin

/usr/X11R6/bin

/root/bin 순서로 검색하여 실행합니다.

다음은 jbc 라는 사용자의 지령 PATH 를 확인한것입니다.

```
[jbc@dell-rss ~]$ id
uid=500(jbc) gid=500(jbc) groups=500(jbc)
[jbc@dell-rss ~]$ echo $PATH
/usr/local/bin:/bin:/usr/bin:/usr/X11R6/bin:/home/jbc/bin
[jbc@dell-rss ~]$
```

jbc 자가 지령을 실행하였을때 그 지령을 찾는 순서는 실례에서 보여준것과 같습니다.

우에서 확인한 관리자와 일반사용자의 PATH는 《붉은별》봉사기용체계 3.0의 기정설정입니다. 그러나 일반사용자의 PATH를 다음과 같이 설정할것을 권고합니다.

먼저 root 권한으로 가입해서 어떤 등록부를 하나 창조합니다. 실례로 /userbin 이라는 등록부를 만들어서 일반사용자들이 사용할수 있는 아주 제한적이고 꼭 필요한 지령들만을 여기에 보관합니다.

그리고 일반사용자들의 PATH를 앞에서 설정한것처럼 하지 않고 /userbin 에서만 검색하여 사용하도록 설정합니다. 이렇게 하기 위해서는 체계설치직후에 root권한으로 가입해서 /userbin이라는 등록부를 창조하고 거기에 일반사용자들이 사용할수 있는 아주 제한적이고 꼭 필요한 지령들만을 보관합니다.

다음 /home/kim/.bash_profile의 PATH값을 PATH=$PATH:$HOME/bin설정을 PATH=/userbin 으로 수정합니다. 이것을 확인하기 위하여 root가입을 탈퇴하고 다시 kim사용자로 가입해서 다음의 지령을 입력합니다.

```
[kim@localhost ~]$ echo $PATH
/userbin
[kim@localhost ~]$ su
-bash: su: 지령없음
[kim@localhost ~]$
```

Su지령을 실행하면 지령없음이라는 통보문을 볼수 있습니다.

25. 화일속성으로 화일보안실현

▶ 화일보안을 위한 chattr지령.

여기서는 chattr지령을 리용하여 특정화일에 대한 삭제 및 변경, 추가등을 불가능하게 하는 방법을 설명합니다. 이 지령을 리용하여 삭제 및 변경, 추가를 불가능하게 하는 화일들은 대체로 체계기동화일들입니다. 즉 /etc/rc.d/rc, /etc/rc.d/rc.local, /etc/rc.d/rc.sysinit화일들입니다. 물론 이외에도 chattr지령을 리용하여 다른 중요한 화일들에 대한 속성지정은 얼마든지 할수있습니다.

《붉은별》봉사기용체계 3.0의 화일속성내용은 일반 지령으로 확인할수 없으며 오직 lsattr로만 가능합니다. 《붉은별》봉사기용체계 3.0 체계에는 root권한으로도 삭제되지 않는 화일들이 존재합니다. 그 리유는 이 화일들에

화일삭제가 되지 않도록 속성이 설정되여 있기때문입니다. 이런 경우에 chattr 나 lsattr 지령으로 화일속성을 확인해보아야 합니다.

이런 화일의 속성을 설정하고 제거하는 지령이 chattr 이고 화일에 설정되여 있는 속성을 확인하는 지령이 바로 lsattr 지령입니다.

《붉은별》봉사기용체계 3.0 에는 화일의 권한외에도 속성이라는 개념이 존재합니다. 유능한 봉사기관리자라면 화일의 권한뿐아니라 화일의 속성에 대한 리해도 정확히 가지고 있어야 합니다.

화일의 권한과 속성이 어떻게 다른가?

한마디로 화일의 권한은 ls 지령으로 확인할수 있는 화일의 읽기, 쓰기,실행에 관한 표시를 하지만 화일의 속성은 lsattr 지령으로 확인할수 있는 화일의 변경, 접근, 실행등의 권한을 설정해둔것입니다.

Chattr 의 사용법:

#chattr [-RV] [-v 설정판본] [+-=설정방식] 대상화일들

Lsattr 의 사용법:

#lsattr [-Rvadv] [대상화일들]

chattr 에서 사용하는 [설정방식]은 다음과 같습니다.

+: 지정한 속성을 부합니다. +기호가 사용되면 지정한 속성을 부여한다는 뜻입니다.

-: 지정한 속성을 제거합니다. -기호가 사용되면 지정한 속성을 제거한다는 뜻입니다.

=: 현재 화일이 가지고 있는 그 속성만을 유지합니다.

그리고 chattr 에서의 –RVv 선택항목에 대한 설명은 다음과 같습니다.

-R: 보조등록부이하까지 그 속성을 변경할수 있습니다.

-V: 자세한 출력방식을 제공합니다.

-v : 지정된 화일에 판본을 설정할수 있습니다.

또한 chattr 지령에서 무엇보다 중요한것은 매 속성의 의미를 정확히 파악하는것입니다. Chattr 로 설정할수 있는 화일(등록부)의 속성에는 다음과 같은 것들이 있습니다.

a 속성

해당 화일을 추가만 할수 있습니다. 이 속성은 root만이 속성변경이 가능합니다. 화일보안을 위해 주로 사용되는 속성으로서 /var/log/messages와 같은 기록화일에 적용합니다.

c속성

이 속성이 설정된 화일은 핵심부에 의해 디스크상에 자동적으로 압축된 상태로 보관됩니다. 화일을 읽기하는 경우에는 압축을 해제한 상태로 되돌려주며 쓰기때에는 디스크에 보관하기 전에 화일을 압축합니다.

d속성

이 속성이 설정된 화일은 dump로 여벌복사되지 않습니다.

i속성

이 속성이 지정되여 있으면 해당 화일의 변경, 삭제, 이름변경뿐아니라 화일추가 및 련결화일도 만들수 없습니다. 변경추가가 거의 없는 기동관련화일들에 설정하면 기동이 되지 않는 문제로 인한 체계고장를 줄일수 있습니다. a속성과 함께 많이 사용하는 속성입니다.

s속성

이 속성이 설정된 화일은 화일삭제가 될 경우에 해당 블로크가 모두 0이 되고 디스크에 다시 쓰기가 발생합니다.

S속성

이 속성이 설정된 화일은 변경이 될 경우에 디스크동기화의 효과를 그대로 유지합니다.

u속성

이 속성을 가진 화일이 삭제되였을 경우에 그 내용이 보관되며 삭제되기전의 자료로 복구가 가능합니다.

따라서 chattr로 화일과 등록부의 속성을 지정하는 기본리유는 바로 허가되지 않은 사용자가 화일의 변경을 못하게 설정함으로서 화일보안을 실현하자는데 있습니다. 여기서 주의할것은 a, i, j속성은 root만이 설정할수 있다는것입니다. 일반사용자는 자기소유의 화일이라도 이 속성은 설정할수 없습니다. 만약 사용자가 자기소유의 화일에 이런 속성을 설정하려고 한다면 오유통보문이 출력되면서 설정되지 않습니다.

▶ 화일의 변경,삭제,추가를 불가능하게 설정

chattr는 주로 화일속성을 설정하지만 등록부에 대한 속성도 화일과 동일하게 설정할수 있습니다. 그럼 /etc/rc.d/등록부에 존재하는 rc.local 화일을 실례로 설명합니다. 이 화일은 기동프로쎄스의 맨 마지막단계로서 추가설치된 응용프로그람의 실행을 기동시에 자동적으로 실행하기위해 사용하는 화일입니다. 특정화일에 대하여 root도 마음대로 변경할수 없게 하려면 i속성을 설정하면 됩니다. I속성이 설정된 화일은 삭제뿐아니라 변경, 내용추가등이 전혀 불가능합니다.

```
[root@dell-rss rc.d]# lsattr rc.local
------------- rc.local
[root@dell-rss rc.d]# chattr +i rc.local
[root@dell-rss rc.d]# lsattr rc.local
----i-------- rc.local
[root@dell-rss rc.d]# rm -f rc.local
rm: `rc.local'를 제거할수  없습니다.: 명령이 허용되지 않았습니다.
[root@dell-rss rc.d]# █
```

실례에서는 rc.local화일의 속성을 확인하고 i속성을 부여한후 한번 삭제해보았다. 그러나 삭제되지 않았다. i속성을 제거하려면 –i라고 주면됩니다.

▶ 화일삭제는 불가능하지만 내용추가는 가능하게 속성설정.

화일에 a속성이 부여되여 있다면 화일삭제는 불가능하지만 내용추가는 가능하게 할수 있습니다. a속성은 주로 /var/log등록부에 존재하는 기록화일들 즉 messages, secure, maillog화일들에 설정합니다.

```
[root@dell-rss log]# ls -l messages
-rw-------  1 root root 206896  2009 10월 20 19:20 messages
[root@dell-rss log]# chattr +a messages
[root@dell-rss log]# lsattr messages
-----a------- messages
[root@dell-rss log]# █
```

결국 i속성은 《붉은별》봉사기용체계 3.0설치후에 변경사항이 전혀 없는 화일들에 설정하고 a속성은 기록화일들에 사용합니다.

▶ 특정등록부의 모든 화일들과 보조등록부들에 동시에 속성설정.

```
[root@dell-rss home]# ls -lR jbc | more
jbc:
검사합 45136
drwxr-xr-x  2 jbc  jbc     16384  2009 10월 13 15:00 2009.05
drwx------  3 jbc  jbc      4096  2009  5월 30 17:29 Desktop
-rwxr--r--  1 jbc  jbc   1228288  2004  9월 14 06:28 Win98.img
-rwxr--r--  1 jbc  jbc       937  2009  5월 30 00:20 dhcpd.conf
-rwxr--r--  1 jbc  jbc   4056379  2007  9월  6 09:00 initrd.img
-rwxrwxrwx  1 root jbc  38944084  2005  1월  6 09:00 kernel-2.6.
-rwxr--r--  1 jbc  jbc      4538  2007 11월  8 04:09 mba.pxe
-rwxr-xr-x  1 root root    11822  2009  8월 20 14:54 pxelinux.0
-rwxr--r--  1 jbc  jbc   1876069  2007  9월  6 20:19 vmlinuz
-rw-r--r--  1 root root     2799  2009  5월 29 13:27 xorg.conf
```

jbc 등록부안에 있는 모든 화일들과 등록부들에 i속성을 설정합니다.

```
[root@dell-rss home]# chattr -R +i jbc
[root@dell-rss home]# lsattr -R jbc | more
----i-------- jbc/pxelinux.0
----i-------- jbc/kernel-2.6.9-5.EL.src.rpm
----i-------- jbc/dhcpd.conf
----i-------- jbc/xorg.conf
----i-------- jbc/initrd.img
----i-------- jbc/Win98.img
----i-------- jbc/Desktop
```

우의 속성설정을 제거하려면 +i대신 –i를 실행합니다.

- 화일의 여러가지 속성을 한번에 설정.

어떤 화일에 a, i, s, S, u속성 5개를 동시에 설정합니다.

```
[root@dell-rss jbc]# ls -l file1
-rw-r--r--  1 root root 0  2009 10월 20 19:42 file1
[root@dell-rss jbc]# lsattr file1
------------- file1
[root@dell-rss jbc]# chattr +aisSu file1
[root@dell-rss jbc]# lsattr file1
suS-ia------- file1
[root@dell-rss jbc]# █
```

26. 하드디스크의 물리적인 고장발생과 대책

디스크의 물리적인 고장으로 체계가 꺼지는 경우는 대채로 하드디스크의 오유블로크때문입니다. 이런경우 여벌복사를 해두었다면 디스크를 교체하여 복구할수도 있지만 이 작업역시 3~4시간동안 체계를 정지시켜야 하므로 손실은 피할수 없습니다.

그러면 디스크를 여벌복사해두지 않았을 경우 해결책은 전문가들에 의뢰하는것입니다. 이런 경우가 최악의 경우라고 할수 있습니다. 디스크의 물리적인 문제를 해결하기 위하여 RIAD 로 구성하기도하고 디스크동기화를 하기도 합니다. 그러지만 이런 방법들이 최종적으로 해결책이 될수는 없습니다. 그렇다고 봉사기관리자들이 디스크고장가 발생하지 않기만을 기대할수도 없습니다.

디스크의 물리적인 고장이라면 대부분 디스크의 오유블로크 문제입니다. 디스크에 오유블르크가 존재하면 언제 체계가 꺼질지 알수 없습니다.

디스크의 물리적인 문제가 발생하지 않기만을 기다릴것이 아니라 주기적으로 점검을 해서 이런 문제가 발생하기 전에 대책을 세우는것이 현시점에서는 가장 좋은 해결책이라고 할수 있습니다.

E2fsck 지령의 선택항목에는 badblocks 를 실행하여 오유블로크를 찾은 다음 디스크의 오유블로크 inode 에 추가하여 mark 되여 있는 오유블로크를 사용하지 못하도록 하는 방법이 있습니다.

-c 선택항목으로 불량블로크표시가 가능하며 최고 1 년에 2 회이상은 불량블로크를 점검하여 불량블로크가 존재할 경우에는 이를 표식하여 사용하지 못하게 설정해야 합니다.

다음은 e2fsck 를 리용하여 /dev/hda1 화일체계안에 불량블로크가 있는가를 찾아서 만약 존재한다면 불량블로크 inode 에 표식하는 작업입니다.

참고로 주의할것은 현재 탑재되여있는 상태에서 e2fsck 로 불량블로크표식작업을 하게 되면 WARNING!!통보문이 출력되면서 화일체계가 손상될수 있습니다. 따라서 e2fsck 사용시에는 반드시 탑재해제된 상태에서 작업을 해야 합니다.

```
[root@dell4-jbc /]# e2fsck -cv /dev/hda1
e2fsck 1.35 (28-Feb-2004)
/dev/hda1 is mounted.

WARNING!!!  Running e2fsck on a mounted filesystem may cause
SEVERE filesystem damage.

Do you really want to continue (y/n)? yes

/: recovering journal
Clearing orphaned inode 613864 (uid=0, gid=0, mode=0140755, size=0)
Checking for bad blocks (read-only test): done
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Entry '172.29.88.57.log' in /var/log/samba (256888) has deleted/unused inode 258294.  Clear<y>?
 yes

Entry 'bau-com.log' in /var/log/samba (256888) has deleted/unused inode 258295.  Clear<y>? yes

Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
Block bitmap differences:  +272611 -272647
Fix<y>? yes


/: ***** FILE SYSTEM WAS MODIFIED *****
/: ***** REBOOT LINUX *****

  141614 inodes used (13%)
    2624 non-contiguous inodes (1.9%)
         # of inodes with ind/dind/tind blocks: 6524/26/0
  704137 blocks used (68%)
       0 bad blocks
       1 large file

  120710 regular files
   12338 directories
       0 character device files
       0 block device files
       1 fifo
    3543 links
    8538 symbolic links (8494 fast symbolic links)
      18 sockets
--------
  145148 files
[root@dell4-jbc /]# █
```

이렇게 불량블로크를 찾아서 표식한다면 그이후부터는 표식된 블로크에 자료를 저장하지 못하게 됩니다.

이 작업에서 주의할것은 현재 사용중인 디스크를 대상으로 불량블로크표식작업을 절대로 해서는 안된다는것입니다. 그리고 가능한 디스크불량블로크를 주기적으로 점검할 때는 cron을 리용하여 자동화시키는것도 좋은 방법으로 되지만 관리자자신이 직접 조작탁에서 작업하는것이 더 좋습니다.

27. 화일을 삭제하지 않고 용량만 0 으로 설정

봉사기를 관리하다보면 access_log 라는 웨브기록화일이나 특정기록화일의 크기가 너무 커져서 체계속도가 현저하게 느려지거나 화일체계가 여유가 없어 고장이 발생하는 경우가 종종 발생합니다.

이에 대해서는 find 나 ls 와 같은 지령을 리용하여 이상한 용량을 가진 화일을 주기적으로 찾아서 확인하는 작업을 해야 합니다. 여기서는 특정화일을 삭제하지 않고 용량만을 완전히 0 으로 만드는 아주 간단한 방법에 대하여 봅니다.

실례로 /etc/httpd/~log 등록부는 련결등록부서 실지 등록부는 /var/log/httpd 입니다. 이 등록부의 기록화일의 용량이 지내 커져서 이 화일의 용량을 줄여야 하는 정황이라고 가정합니다. 이 경우 다음과 같이 합니다.

사용형식 : cat /dev/null > 화일명.

cat /dev/null > /var/log/httpd/access_log

이 지령으로 access_log 화일의 크기를 0 으로 만들었다. 여기서 /dev/null 은 null 장치를 의미하는것으로서 회수통으로 볼수 있습니다. 즉 여기에는 어떠한 내용도 보관되지 않습니다.

28. 디스크사용량점검지령 du

du 는 《Disk Uasge》의 략자입니다. 화일 및 등록부의 사용량을 확인할 때 사용하는 지령입니다.

이 지령은 df 지령과 함께 《붉은별》봉사기용체계 3.0 에서 디스크의 사용량을 점검하고 검사하는 가장 실무적인 지령입니다. 즉 df 지령이 구획(화일체계)단위의 디스크사용량을 점검한다면 du 는 특정 등록부 또는 화일을 단위로하여 그 용량을 확인하는 지령입니다.

df 와 du 는 사용량을 점검한다는 용도는 같지만 그 대상은 각각 다르므로 반드시 함께 습득해야 목적에 부합되는 사용량을 정확하게 점검할수 있습니다. 다시말하여 du 는 현재 등록부의 용량뿐아니라 현재 등록부의 보조등록부 및 화일들을 모두 함께 계산하여 용량을 표시합니다.

사용형식: du [선택항목]…[화일][등록부]

특정등록부안에 존재하는 화일들의 개별용량을 확인하려고 할 때 다음과 같이 《du 등록부명》이라고 하면 지정한 등록부안에 존재하는 모든 화일의 용량을 kbyte 단위로 표시합니다.

```
[root@localhost tftpboot]# du /tftpboot
56      /tftpboot/linux-install/msgs
8       /tftpboot/linux-install/pxelinux.cfg
88      /tftpboot/linux-install
1352    /tftpboot
[root@localhost tftpboot]# █
```

그러나 화일이 많은 경우에 한 화면에 다 현시할수 없기때문에 요구하는 정보를 확인하기 어렵습니다. 따라서 이번에는 전체 용량을 정리하여 보는 실례를 봅니다.

1) 특정등록부의 전체용량 점검.

du지령사용시 "-s(summary)"선택항목을 리용하면 지정된 등록부안에 있는 모든 화일과 보조등록부들의 용량을 모두 합친 전체 용량을 표시합니다.

```
[root@localhost tftpboot]# du -s
42304   /etc
[root@localhost tftpboot]# █
```

다음은 전체용량을 단위까지 붙혀서 현시하는 방법을 봅니다.

전체 용량을 단위까지 현시하는 du지령의 선택항목은 "-sh"입니다. 여기서 "-h(human-readable)"선택항목은 단위까지 표시하게 하는 du 지령의 선택항목으로서 KB, MB, GB등의 용량표시를 합니다. 즉 "-h"선택항목은 human-readable의 략자로서 사람이 좀 더 읽기 편리하게 해준다는 의미입니다.

```
[root@localhost tftpboot]# du -sh /etc
42M     /etc
[root@localhost tftpboot]# █
```

이번에는 좀 더 현실적인 실례를 봅시다.

봉사기관리에서 뿌리등록부밑에 존재하는 매 등록부들의 개별사용량을 확인하거나 사용량보고서를 작성해야 할 때가 있습니다. 이때 다음과 같은 지령으로 개별등록부의 사용량을 간편하게 확인할수 있습니다.

```
[root@localhost tftpboot]# du -sh /*
448K    /000
4.0K    /beam-setup.out
5.2M    /bin
12M     /boot
216K    /dev
42M     /etc
109M    /home
8.0K    /initrd
121M    /lib
16K     /lost+found
16K     /media
8.0K    /misc
592K    /mnt
128M    /opt
197M    /proc
4.0K    /result
498M    /root
14M     /sbin
8.0K    /selinux
8.0K    /srv
0       /sys
1.4M    /tftpboot
5.4M    /tmp
```

2) 일반사용자식별자의 홈등록부의 전체 디스크사용량점검.

개별사용자가 자기자신이 사용하는 사용자식별자의 전체 용량을 확인하려고 할 때에는 다음과 같이 합니다. ssh로 봉사기에 가입한 후에 du –sh ~user라고 하면 현재 자기가 사용하는 사용자식별자의 전체용량을 확인할수 있습니다.

```
[root@c5 /]# du -sh ~kim
44K     /home/kim
[root@c5 /]#
```

29. 화일체계별 디스크사용량을 점검하는 df지령

df는 "Disk Free"의 략자로서 현재 사용중인 화일체계의 전체용량, 사용한 용량, 사용가능한 용량, 사용률, 탑재정보등을 현시합니다.

봉사기고장의 주요 원인으로 될수 있는 "File System Full"을 방지하기 위하여 봉사기관리자의 중요 업무중의 하나가 바로 화일체계사용량점검입니다. 이때 화일체계의 사용량점검을 위해 사용하는 지령이 바로 df지령입니다.

또한 df지령은 /etc/fstab화일에서 화일체사용자식별자보를 참조하고 /etc/mtab에서 탑재된 정보를 참조합니다. 그리고 기본표시용량단위는 KB이며 주로 봉

사기관리자(root)가 사용하는 지령입니다. 봉사기관리자들은 이 지령을 너무 간단하게만 사용합니다.

그러나 df지령만큼 봉사기관리자들에게 큰 도움을 주는 지령은 많지 못하다는 것을 인식해야 합니다.

- 현재 봉사기의 디스크사용량을 구획별로 확인

화일체계사용량을 확인하려면 간단히 df라고 하면 됩니다.

```
[jbc@acer3-server ~]$ df
화일체계              1K-blocks      Used Available Use% Mounted on
/dev/hdc3               4996760   1602992   3139944  34% /
none                      90528         0     90528   0% /dev/shm
/dev/hda2               4032124   2804244   1023052  74% /mnt/hda2
/dev/hda5              39677408   2761240  34867884   8% /mnt/hda5
/dev/hda6              27456092  18780480   7541748  72% /mnt/hda6
/dev/hdc2              31133528  11552368  18295320  39% /mnt/hdc2
/dev/hdc5              37341748  15335052  20464460  43% /mnt/hdc5
[jbc@acer3-server ~]$ █
```

- 첫째마당은 화일체계장치명.
- 둘째마당은 매 화일체계에 할당된 용량.
- 셋째마당은 사용된 용량.
- 넷째마당은 사용가능한 용량.
- 다섯째마당은 현재 할당된 용량에 대한 사용된 용량의 %수.
- 여섯째마당은 매 화일체계의 탑재위치.

- 디스크용량을 구획별로 확인할 때 용량을 KB로 현시.

```
[jbc@acer3-server ~]$ df -k
화일체계              1K-blocks      Used Available Use% Mounted on
/dev/hdc3               4996760   1602992   3139944  34% /
none                      90528         0     90528   0% /dev/shm
/dev/hda2               4032124   2804244   1023052  74% /mnt/hda2
/dev/hda5              39677408   2761240  34867884   8% /mnt/hda5
/dev/hda6              27456092  18780480   7541748  72% /mnt/hda6
/dev/hdc2              31133528  11552368  18295320  39% /mnt/hdc2
/dev/hdc5              37341748  15335052  20464460  43% /mnt/hdc5
```

우의 결과와 갈다는것을 알수 있습니다. 왜냐면 df지령의 단위가 기정으로 KB이기때문입니다.

- 디스크사용량을 구획별로 확인할 때 용량을 MB로 현시.

```
[jbc@acer3-server ~]$ df -m
화일체계            1M-blocks      Used Available Use% Mounted on
/dev/hdc3                4880      1566      3067  34% /
none                       89         0        89   0% /dev/shm
/dev/hda2                3938      2739      1000  74% /mnt/hda2
/dev/hda5               38748      2697     34051   8% /mnt/hda5
/dev/hda6               26813     18341      7365  72% /mnt/hda6
/dev/hdc2               30404     11282     17867  39% /mnt/hdc2
/dev/hdc5               36467     14976     19985  43% /mnt/hdc5
[jbc@acer3-server ~]$ █
```

- 디스크사용량을 구획별로 확인할 때 가장 적당한 용량단위표시.

```
[jbc@acer3-server ~]$ df -h
화일체계            Size  Used Avail Use% Mounted on
/dev/hdc3            4.8G  1.6G  3.0G  34% /
none                  89M     0   89M   0% /dev/shm
/dev/hda2            3.9G  2.7G 1000M  74% /mnt/hda2
/dev/hda5             38G  2.7G   34G   8% /mnt/hda5
/dev/hda6             27G   18G  7.2G  72% /mnt/hda6
/dev/hdc2             30G   12G   18G  39% /mnt/hdc2
/dev/hdc5             36G   15G   20G  43% /mnt/hdc5
[jbc@acer3-server ~]$ █
```

- 디스크용량 확인시 화일체계크기가 0 인것까지 모두 확인.

선택항목 –a 를 리용하면 화일체계의 크기 0 인것까지 모든 화일체계를 확인할수 있습니다.

```
[root@localhost ~]# df -a
화일체계            1K-blocks      Used Available Use% Mounted on
/dev/hda1             16002200   3524104  11665208  24% /
none                         0         0         0   -  /proc
none                         0         0         0   -  /sys
none                         0         0         0   -  /dev/pts
none                     95988         0     95988   0% /dev/shm
none                         0         0         0   -  /proc/sys/fs/binfmt_misc
sunrpc                       0         0         0   -  /var/lib/nfs/rpc_pipefs
[root@localhost ~]# █
```

앞에서 볼수 없었던 화일체계들인 /proc, /proc/sys/fs/binfmt_misc, /var/lib/nfs/rpc_pipsfs, /dev/pts, /sys, dev/pts 들이 현시됩니다. 이 화일체계들은 모두 할당용량, 사용량, 빈용량등이 모두 0 으로 되여있었기 때문에 앞에서는 제외되였던것입니다.

- 디스크사용량을 화일체계의 종류와 함께 표시.

```
[root@localhost ~]# df -T
화일체계    형태   1K-blocks      Used Available Use% Mounted on
/dev/hda1     ext3    16002200   3524112  11665200  24% /
none         tmpfs       95988         0     95988   0% /dev/shm
[root@localhost ~]# █
```

- 특정 화일체계의 종류만을 대상으로 디스크사용량표시.

```
[root@localhost ~]# df -t ext3
화일체계            1K-blocks      Used Available Use% Mounted on
/dev/hda1            16002200   3524112  11665200  24% /
[root@localhost ~]#
```

- 특정 화일체계의 종류를 제외한 디스크사용량표시.

```
[root@localhost ~]# df -x ext3
화일체계            1K-blocks      Used Available Use% Mounted on
none                    95988         0     95988   0% /dev/shm
[root@localhost ~]#
```

30. 화일의 소유자와 그룹변경지령 chown.

Chown 지령은 Change Owner 략자로서 화일이나 등록부의 소유자와 소유그룹을 변경할 때 리용하는 지령입니다. 소유자와 소유그룹은 세번째마당과 네번째마당입니다.

```
[root@localhost ~]# ls -l
검사합 1044      3번째마당 4번째마당
drwx------    3 root root    4096  2008  2월  1 18:36 Desktop
drwx------    7 root root    4096  2008  3월 31 11:22 Mail
-rw-r--r--    1 root root     837  2008  2월  1 16:47 anaconda-ks.cfg
-rw-r--r--    1 root root   40101  2008  2월  1 16:47 install.log
-rw-r--r--    1 root root    8221  2008  2월  1 16:47 install.log.syslog
-rw-r--r--    1 root root  978851  2008 10월  4 22:20 oldflashplugins.ta
r.gz
-rw-r--r--    1 root root    1023  2008 12월 20 10:37 vpd.properties
drwxr-xr-x   17 root root    4096  2008 10월  4 22:18 work
[root@localhost ~]#
```

사용형식

chown [-Rcfv][--recursive][--changes][--help][--version][--silent][--quiet][--verbose][user][:,][group] 화일…

1) 특정사용자의 소유자와 그룹변경.

먼저 간단한 실례로서 file1 의 소유자를 변갱합니다. 즉 ls 로 확인한 결과 file1 의 소유자는 root 로 되여있습니다. 이것을 bible 소유자로 만듭니다.

```
[root@localhost test]# ls -l
검사합 4
drwxr-xr-x  2 root root 4096  2009  1월  8 12:41 dir1
-rw-r--r--  1 root root    0  2009  1월  8 12:41 file1
-rw-r--r--  1 root root    0  2009  1월  8 12:42 file2
[root@localhost test]# chown bible file1
[root@localhost test]# ls -l
검사합 4
drwxr-xr-x  2 root  root 4096  2009  1월  8 12:41 dir1
-rw-r--r--  1 bible root    0  2009  1월  8 12:41 file1
-rw-r--r--  1 root  root    0  2009  1월  8 12:42 file2
```

물론 이 지령이 허용되자면 화일에 대한 소유권이 존재해야 합니다. 아무런 화일이나 등록부의 소유자를 변경할수있는것은 아닙니다.

2) 특정화일의 소유자와 소유그룹을 동시에 변경.

앞에서는 chown 지령으로 화일의 소유자만을 변경하였습니다. 이번에는 화일의 소유자와 그룹소유자를 동시에 변경합니다.

```
[root@localhost test]# ls -l
검사합 4
drwxr-xr-x  2 root  root 4096  2009  1월  8 12:41 dir1
-rw-r--r--  1 bible root    0  2009  1월  8 12:41 file1
-rw-r--r--  1 root  root    0  2009  1월  8 12:42 file2
[root@localhost test]# chown bible:bible2 file2
[root@localhost test]# ls -l
검사합 4
drwxr-xr-x  2 root  root    4096  2009  1월  8 12:41 dir1
-rw-r--r--  1 bible root       0  2009  1월  8 12:41 file1
-rw-r--r--  1 bible bible2     0  2009  1월  8 12:42 file2
```

우의 실례는 file2 이라는 화일의 소유자를 root 에서 bible 로 변경하였으며 소유그룹을 root 에서 bible2 로 변경한 실례입니다. 즉 chown 지령에서 bible:bible2 의 의미는 대상화일의 소유자를 bible 로하고 소유그룹을 bible2 로 설정하라는 의미입니다.

- 특정 등록부의 소유자와 소유그룹 동시에 변경.

```
[root@localhost test]# ls -l
검사합 4
drwxr-xr-x  2 root  root   4096  2009  1월  8 12:41 dir1
-rw-r--r--  1 bible root      0  2009  1월  8 12:41 file1
-rw-r--r--  1 bible bible2    0  2009  1월  8 12:42 file2
[root@localhost test]# chown bible1:bible2 dir1
[root@localhost test]# ls -l
검사합 4
drwxr-xr-x  2 bible1 bible2 4096  2009  1월  8 12:41 dir1
-rw-r--r--  1 bible  root      0  2009  1월  8 12:41 file1
-rw-r--r--  1 bible  bible2    0  2009  1월  8 12:42 file2
[root@localhost test]#
```

이 실례는 dir1 라는 등록부의 소유자를 root 에서 bible1 로 변경하고 소유그룹을 root 에서 bible2 로 변경한 실례입니다.

- 특정등록부안의 모든 화일, 등록부의 소유자(그룹)을 동시에 변경.

봉사기작업시 특정 등록부안의 모든 화일과 등록부들을 특정 소유자와 소유그룹으로 변경해야 하는 경우가 있습니다. 례를 들어 웨브에서 자료등록부의 소유자와 소유그룹을 nobody 와 nobody 로 해주어야 할경우가 종종 발생합니다. 즉 apache 에서 특정 등록부안에 화일을 저장하려면 읽기, 쓰기권한이 있어야 합니다. 그런데 등록부의 소유자와 그룹을 nobody 로 설정하면 간단히 해결할수 있으므로 이런 작업이 필요합니다.

특정등록부의 모든 화일과 보조등록부까지 소유자와 그룹을 한번에 변경하려면 다음과 같이 –R 선택항목을 리용할수 있습니다.

```
[root@localhost jbc]# chown -R nobody:nobody test
[root@localhost jbc]# ls
Desktop  test
[root@localhost jbc]# ls -l
검사합 8
drwx------  3 jbc    users  4096  2008  2월  6 12:31 Desktop
drwxr-xr-x  3 nobody nobody 4096  2009  1월  8 12:42 test
[root@localhost jbc]#
```

3) 특정 등록부의 특정화일들에 대하여서만 소유자와 그룹변경.

많이 사용하지는 않지만 반드시 알아야 할 지령입니다. 즉 특정등록부안에 많은 화일들이 함께 들어있고 또한 그 등록부에는 한사람의 소유로 되여있는것이 아니라 여러 사람의 소유로 된 화일들이 함께 들어가 있습니다. 일반적으로 한 등록부안에 있는 화일들은 동일한 소유자로 되여 있다, 그러나 같은 등록부안의 화일들의 소유자가 각각 다른 경우도 있습니다. 그런 등록부는 /tmp 등록부입니다.

아래 실례에서는 특정등록부안에 존재하는 많은 화일중에서 특정사용자의 소유로 되여있는 화일들만 변경하는 방법입니다.

 # chown -R jbc:webhost uploads --from=nobody:nobody

이것은 uploads 라는 등록부안에 있는 화일들중 소유자가 nobody 이고 그룹이 nobody 로 되여있는 화일들의 소유자를 jbc 로 변경하고 그룹을 webhost 로 변경하는 실례입니다.

31. 화일권한을 설정하는 chmod 지령

여기서는 화일권한과 화일의 속성에 대하여 설명합니다. 일반적으로 화일을 규정하고 제한하는 방법은 여러가지가 있습니다. 그러나 봉사기관리자들은 화일권한뿐아니라 화일의 속성까지도 알아야 하며 SetUID, SetGID, StickyBit 에 대하여서도 알아야 화일을 모두 파악했다고 말할수 있습니다.

- 화일과 등록부의 권한(permission)

chmod 는 화일과 등록부의 권한을 설정하는 지령입니다. 《붉은별》봉사기용체계 3.0 의 가장 기본적인 지령으로서 《붉은별》봉사기용체계 3.0 사용자라면 누구나 알고 있어야 할 지령입니다.

권한이란 특정화일이나 등록부에 대하여 읽기, 쓰기, 삭제등을 설정하는 권한으로서 다중사용자조작체계에서 화일의 접근권한과 보호들을 위하여 반드시 필요한것입니다. 흔히 웨브홈페지를 열람할 때 웨브문서화일의 권한이 설정되여있지 않으면 《이 문서는 허용되지 않았습니다.》라는 통보문이 현시됩니다. 이 원인은 거의 대부분 웨브페지화일의 권한이 허용되여있지 않기 때문입니다.

홈페지를 만들어서 《붉은별》봉사기용체계 3.0 에 적재한 후 사용자들이 사용할수있게 화일의 권한설정을 설정해야 합니다. 화일의 권한종류에는 다음과 같이 다섯가지가 있습니다.

표 1. 화일,등록부권한의 종류

권한	의미	화일	등록부
r	읽기권한	화일읽기.	
w	쓰기권한	화일 보관, 삭제.	
x	실행권한	화일실행.	

s	SetUID, SetGID 권한	화일소유자(SetUID)권한, 그룹소유자 (SetGID)권한으로 실행.
T	Sticky Bit	공유등록부로 사용됨.

우의 실례에서 같은 권한일경우에도 화일에 대한 의미와 등록부에 대한 의미가 좀 차이난다는것을 알수 있습니다.

가능한 선택항목들.

-c : 옳게 변경된 화일들만 –v 선택항목을 적용하여 상세히 보여줍니다.

-f : 가능한 불필요한 통보문은 보여 주지 않고 간단하게 보여줍니다.

-v : 실행과정을 자세히 보여줍니다.

-R : 등록부와 그안에 존재하는 보조등록부들까지 모두 적용합니다.

화일의 권한을 정확히 리해하기 위해서는 2 진수, 8 진수, 10 진수관계를 잘 알아야 합니다.

표 2. 권한의 표기법과 의미

2 진수	8 진수	표시되는 권한	의미
000	0	---	아무런 권한없음
001	1	--x	실행권한
010	2	-w-	쓰기권한
011	3	-wx	쓰기, 실행권한
100	4	r--	읽기권한
101	5	r-x	읽기, 실행권한
110	6	rw-	읽기,쓰기권한
111	7	rwx	읽기,쓰기,실행

보다 정확한 설명을 위하여 아래와 같이 《ls –l》 지령의 결과를 봅시다.

```
[root@localhost jbc]# ls -l
검사합 8
drwx------   3 jbc     users   4096  2008  2월  6 12:31 Desktop
drwxr-xr-x   3 nobody  nobody  4096  2009  1월  8 12:42 test
[root@localhost jbc]# █
```

우의 두번째행의 정보는 다음과 같습니다.

drwx------ 3 nobody nobody 4096 2009 1 월 8 12:42 test

– 화일권한 : drwx-----

- 화일명 : desktop
- 화일소유자 : jbc
- 그룹소유자 : users
- 화일크기 : 4096
- 화일최종변경시간 : 2009 년 1 월 8 일 12 시 42 분

우와 같은 정보에서 권한정보를 보면 다음과 같습니다.

d	rwx	---	---
ㄱ. 화일형태	ㄴ. 소유자권한.	ㄷ. 그룹권한	ㄹ. 일반다른사용자권한

ㄱ. 화일형태.

이 위치에는 다음과 같은 문자들이 설정될수 있으며 그 의미는 다음과 같습니다.

- : 일반화일을 의미.

b : 블로크장치화일(Block Special File)을 의미.(례 /dev/sda)

c : 문자장치화일(Character Special File)을 의미(례 /dev/console)

d : 등록부를 의미하며 등록부도 하나의 특수화일로 취급.

l : 련결화일을 의미.

p : pipe 화일을 의미.

s : 소케트화일을 의미.

ㄴ. 소유자권한

여기에서는 8 가지 경우로 설정될수있으며 그 의미는 다음과 같습니다.

--- : 화일의 소유자에게 아무런 권한이 없음.

--x : 화일의 소유자에게 실행권한만 있음.

-w- : 화일의 소유자에게 쓰기권한만 있음.

-wx : 화일의 소유자에게 쓰기, 실행권한만 있음.

r-- : 화일의 소유자에게 읽기권한만 있음.

r-x : 화일의 소유자에게 읽기, 실행권한만 있음.

rw- : 화일의 소유자에게 읽기, 쓰기권한만 있음.

rwx : 화일의 소유자에게 읽기, 쓰기, 실행권한 모두 있음.

그룹권한, 일반 다른사용자권한은 소유자권한과 의미가 같습니다.

화일의 권한을 설정하는 방법은 두가지가 있습니다.

첫번째방법은 8진수 수자를 지정하여 설정하는 방법입니다.
례 chmod 755 a_file
화일소유자에게 읽기, 쓰기, 실행권한을 설정하고 그룹소유자에게는 읽기, 실행권한만 부여하고 다른 소유자에게는 읽기, 실행권한만 부여한 실례입니다.
둘째방법은 특정문자를 리용한 권한설정방법입니다.
례 #chmod o+rw a_file
다른 사용자에게는 읽기과 쓰기권한을 부여하였습니다.
리용하는 특정문자들에는 다음과 같은것들이 있습니다.
u : 소유자를 의미
g : 그룹을 의미.
o : 다른 사용자를 의미.
a : 모두를 의미합니다.
이 문자와 함께 +기호가 사용되면 《권한을 부여합니다.》라는 의미이며 《-》부호가 사용되면 권한을 삭제한다는 의미입니다.

- 8진수로 화일의 권한설정.

chmod 755 testfile
화일소유자에게 읽기, 쓰기, 실행권한을 부여하고 그룹사용자와 다른 사용자에게는 읽기, 실행권한만 부여하였습니다. 이 설정은 웨브문서화일들에 적용하는 일반적권한설정방법입니다.
chmod 644 testfile
화일소유자에게 읽기, 쓰기권한을 부여하고 그룹사용자와 다른 사용자에게는 읽기권한만 부여하였습니다. 이 설정도 역시 웨브문서화일들에 적용하는 일반적권한설정방법입니다.
chmod 700 testfile
화일소유자에게 읽기, 쓰기, 실행권한을 부여하고 그룹사용자와 다른 사용자에게는 아무런 권한도 부여하지 않았다.. 이 설정은 보안이 요구되는 화일들에 설정하는 일반적권한설정방법입니다.

- 특정문자로 권한설정.

chmod a+r testfile

모든 사용자에게 읽기권한만 부여하였습니다.

chmod a+w testfile

모든 사용자에게 쓰기권한만 부여하였습니다.

chmod a+x testfile

모든 사용자에게 실행권한만 부여하였습니다.

chmod a-rwx testfile

모든 사용자에게 읽기, 쓰기, 실행권한을 삭제하였습니다.

– 여러개의 화일들과 등록부권한을 동시에 설정.

chmod 755 php*

php 로 시작하는 모든 화일들에 755 권한을 부여하였습니다.

– 특정등록부안의 모든 화일들와 보조등록부권한 설정.

보조등록부안의 모든 화일과 등록부까지도 한번에 동일한 권한을 설정하려면 –R 선택항목을 사용합니다.

Chmod -R 755 www

모든 사용자에게 실행권한만 부여하였습니다.

32. 망보안주사도구 nmap

《붉은별》봉사기용체계 3.0 에서 nmap 는 망보안에서 중요한 역할을 합니다. nmap 를 어떻게 리용하는가에 따라 보안도구로 될수도 있고 해킹도구로 될수도 있습니다.

이 도구를 리용하면 해킹의 첫단계로서 봉사기에서 사용하고 있는 조작체계종류, 판본, 주콤퓨터명, 사용하는 봉사대몬들, 열려있는 포구등을 확인할 수 있습니다.

사용형식 : nmap [scan type][option]<대상봉사기 [IP 주소]>

scan option

-sS : TCP SYN scan

-sT : TCP 련결 scan

-sF –sX –sN : Stealth FIN, Xmas Tree, 또는 Null scan mode

-sP : Ping scaning

-su : UDP scaning

-sO : IP protocol scan

-sI <zombie host[:proberport]> : Idlescan

-sA : ACK scan

-sW : Window scan

-sR : RPC scan

-sL : List scan

▶ nmap 로 국부봉사기주사.

현재 사용하고 있는 붉은별체계의 자체정보를 확인합니다.

```
[root@dell-rss jbc]# nmap -sT -O v localhost

Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2009-10-20 20:10 KST
Failed to resolve given hostname/IP: v.  Note that you can't use '/mask' AND '[1-4,7,100-]' styl
e IP ranges
Insufficient responses for TCP sequencing (1), OS detection may be less accurate
Interesting ports on dell-rss (127.0.0.1):
(The 1651 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
631/tcp   open  ipp
10000/tcp open  snet-sensor-mgmt
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.0 - 2.5.20, Gentoo 1.2 linux (Kernel 2.4.19-gentoo-rc5), Linux 2.4.20, Lin
ux 2.4.20 - 2.4.22 w/grsecurity.org patch, Linux 2.5.25 - 2.6.3 or Gentoo 1.2 Linux 2.4.19 rc1-r
c7)

Nmap run completed -- 1 IP address (1 host up) scanned in 4.030 seconds
[root@dell-rss jbc]#
```

이 실례에서 사용한 선택항목의 의미는 다음과 같습니다.

-sT : TCP connect 에 대한 주사를 합니다.

-O :TCP/IP fingerprinting 을 통하여 지정한 봉사기를 확인합니다.

-v : 주사결과를 상세히 보여줍니다.

우의 주사결과를 분석하면 다음과 같습니다.

- 이 봉사기는 《붉은별》봉사기용체계 3.0 를 사용하고 있습니다.
- 이 봉사기의 핵심부판본은 2.6.3 이상입니다.
- 사용하고 있는 TCP 포구는 22, 25, 80, 111, 139, 443 ,445, 631, 10000 이다

▶ 원격봉사기에 대한 주사

이번에는 국부봉사기가 아닌 원격봉사기를 대상으로 nmap 를 실행합니다.

```
[root@dell-rss jbc]# nmap -sU -O -v 192.168.0.211
```

이 실례는 192.168.0.211 봉사기의 UDP 사용포구를 주사한것입니다.

33. 망지령들에 대한 사용법은 보안의 힘있는 도구

1) ping 지령문(망통신시험지령문)

이 지령문은 망관련의 지령문들가운데서 가장 많이 사용되는것이며 Linux 봉사기관리자라면 반드시 알아두어야 하는것입니다. ping지령문은 지정된 대상주콤퓨터로 ICMP 파케트를 보내여 그 응답을 받은 결과에 의해 망통신상태를 검사확인해보는 지령문입니다.

여기서 중요한것은 ping 이라는 망관련지령문을 리용한 대상주콤퓨터와의 망통신가능여부와 이 시험을 위해 ICMP 통신규약을 사용한다는것입니다.

ping을 리용한 간단한 시험을 해보기로 합시다.

ping 지령문의 구성은 ping 다음에 대상 IP 주소로 되여있으며 아래의 례에서와 같이 입력해줍니다. ping시험을 끝낼 때에는 [Ctrl+C]건을 입력합니다.

```
[root@localhost profile.d]# ping 172.29.88.1
PING 172.29.88.1 (172.29.88.1) 56(84) bytes of data.
64 bytes from 172.29.88.1: icmp_seq=0 ttl=64 time=4.51 ms
64 bytes from 172.29.88.1: icmp_seq=1 ttl=64 time=1.18 ms
64 bytes from 172.29.88.1: icmp_seq=2 ttl=64 time=0.919 ms
64 bytes from 172.29.88.1: icmp_seq=3 ttl=64 time=0.979 ms
64 bytes from 172.29.88.1: icmp_seq=4 ttl=64 time=0.949 ms

--- 172.29.88.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 0.919/1.710/4.514/1.405 ms, pipe 2
[root@localhost profile.d]# █
```

우의 결과는 한번의 ping검사시 사용되는 총 파케트크기가 64B 라는것을 알수 있습니다. ping지령검사때 특별한 선택항목이 사용되지 않으면 한번 검사때 사용하는 파케트크기는 56바이트를 사용합니다. 여기에 8바이트의 ICMP 머리부를 함께 보내므로 총 64바이트가 됩니다. ping을 끝낼때에는 ^C를 사용합니다. 여기서 주의해서 볼것은 매 행의 time값입니다. 이 값이 작을수록 현재 봉사기와 ping검사한 대상 봉사기사이의 통신이 빠르다는것을 알수 있습니다. 즉 time값이 낮을수록 회선상태가 좋다는것을 보여줍니다. ^C 한 후에는 ping검사의 통계값을 보여줍니다. 우의 결과는 파케트를 5개 보내고 5개 받았으며 루실된것은 없고 응답결과의 최소시간은 0.919ms이고 평균시간은 1.710ms이며 최대시간은 4.514ms라는것을 알수 있습니다.

ping지령에는 다음과 같은 선택항목들이 있습니다.

-s : ping 검사시에 사용할 파케트크기설정.

-q : ping 검사결과를 지속적으로 보여주지않고 종합결과만 현시.

-i : ping 검사시 사용할 interval 을 설정 즉 지연시간설정.

-b : ping 검사를 하는 봉사기와 통일한 망에 있는 모든 주콤퓨터로 파케트를 보냄.

-c : ping 검사시에 보낼 파케트수를 지정.

실례 1: -c 와 –s 선택항목을 동시에 리용한 실례입니다.

```
[root@localhost profile.d]# ping -c 3 -s 1000 172.29.88.1
PING 172.29.88.1 (172.29.88.1) 1000(1028) bytes of data.
1008 bytes from 172.29.88.1: icmp_seq=0 ttl=64 time=24.9 ms
1008 bytes from 172.29.88.1: icmp_seq=1 ttl=64 time=1.32 ms
1008 bytes from 172.29.88.1: icmp_seq=2 ttl=64 time=1.54 ms

--- 172.29.88.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.323/9.259/24.913/11.069 ms, pipe 2
[root@localhost profile.d]# █
```

우의 결과에서 "-c 3"선택항목으로 3 번의 ping 검사를 하였으며 "-s 1000" 선택항목에 의해 1 회사용할 파케트크기를 1000 바이트로 지정하여 검사하였습니다. 여기서 한가지 의문은 분명"-s 1000"선택항목으로 파케트크기를 1000 바이트로 설정하였는데 실제 사용된 파케트크기는 1008 바이트가 된것입니다. 이것은 한 파케트마다 ICMP 머러부정보로 8 바이트가 사용되며 "1000byte(송신파케트)+8byte(ICMP 머리부정보)"로 사용되기 때문입니다.

실례 2 : -q 선택항목을 사용한 실례입니다. 이 경우에는 검사한 내용을 실시간적으로 보여주지 않고 검사완료시에만 그 결과만을 보여줍니다.

```
[root@localhost profile.d]# ping 172.29.88.1 -q
PING 172.29.88.1 (172.29.88.1) 56(84) bytes of data.

--- 172.29.88.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 0.764/1.107/1.666/0.326 ms, pipe 2
[root@localhost profile.d]# █
```

실례 3: -s 선택항목을 사용하여 파케트크기를 5000 으로 하여 검사한것입니다. 사실 파케트크기를 크게 하면 Dos 공격으로 오해 받을수 있기때문에 이것은 례외적인 검사입니다.

```
[root@localhost profile.d]# ping -s 5000 172.29.88.10
PING 172.29.88.10 (172.29.88.10) 5000(5028) bytes of data.
5008 bytes from 172.29.88.10: icmp_seq=1 ttl=128 time=3.23 ms
5008 bytes from 172.29.88.10: icmp_seq=2 ttl=128 time=1.90 ms
5008 bytes from 172.29.88.10: icmp_seq=3 ttl=128 time=2.46 ms

--- 172.29.88.10 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3001ms
rtt min/avg/max/mdev = 1.907/2.533/3.232/0.543 ms, pipe 2
[root@localhost profile.d]#
```

2) 망경로조종표를 관리하는 route 지령

이 지령은 망의 기본기령으로서 봉사기관리자가 필수적으로 알아야할 지령입니다.

이 지령은 현재 사용중인 봉사기의 경로를 설정하기 위한것으로 특정망대변무에 경로기정보를 설정하는 지령입니다.

만약 봉사기를 경로기로 사용하려 한다면 두개이상의 망대면부가 존재할것입니다. 이 경우 매개 망대면부의 경로기경로를 설정해주야야 하는데 이 경로기경로설정을 route 라는 지령으로 설정합니다.

route 의 가장 기본적인 례로서 현재 봉소기의 기본게이트웨이를 설정하는 방법을 봅니다. 먼저 eth0 라는 망대면부에 기본경로기를 설정하는 방법입니다. 즉 특정 망대면부에 기본경로기를 설정하는 형식은 다음과 같습니다.

형식: route add default gw 경로기 IP 주소 dev 망대면부장치명.

우와 같이 설정된 후에는 아래와 같이 “route”를 실행하여 기본경로기가 경로기표에 정상적으로 설정되였는가를 확인해보아야 합니다.

```
[root@localhost profile.d]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
172.29.88.0     *               255.255.248.0   U     0      0        0 eth0
169.254.0.0     *               255.255.0.0     U     0      0        0 eth0
default         172.29.88.1     0.0.0.0         UG    0      0        0 eth0
[root@localhost profile.d]#
```

우의 결과중에 마지막행의 의미는 다음과 같습니다. 현재 봉사기가 외부와 통신을 할 때에는 172.29.88.1 이라는 경로기를 리용합니다. 즉 동일한 망이 아닌 외부망과 통신을 할 때의 모든 파케트들은 모두 이 경로기를 리용한다는 의미입니다.

우와 같은 설정이 정상적으로 되여있다면 이 봉사기는 외부망와 통신할수 있습니다.

다음은 현재 체계와 통신이 가능하도록하는 망통신경로를 추가하는 실례입니다. 즉 현재 체계의 특정망대면부네 특정망경로를 인식하도록 망마스크를 설정하는 실례입니다.

형식:

route add –net 망 IP주소 netmask 망마스크 dev 망대면부장치명.

```
[root@localhost profile.d]# route add -net 172.29.81.0 netmask 255.255.255.0 dev eth1
[root@localhost profile.d]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
172.29.81.0     *               255.255.255.0   U     0      0        0 eth1
172.29.88.0     *               255.255.248.0   U     0      0        0 eth0
169.254.0.0     *               255.255.0.0     U     0      0        0 eth0
default         172.29.88.1     0.0.0.0         UG    0      0        0 eth0
[root@localhost profile.d]# █
```

우의 설정은 172.29.81.0 망과의 모든 통신파케트는 eth1 이라는 망대면부를 통하여 진행하겠다는 의미입니다. 설정한 후에는 route 지령으로 현재 체계의 경로조종표를 확인합니다. 우의 결과에서 붉은색부분이 route 지령에 의하여 생성된 통신경로입니다. 즉 이 봉사기는 172.29.81.0 망과 통신할 때는 eth1 망대면부를 통하여 진행되게 됩니다.

3) 망상태를 점검하는 netstat 지령

netstat 지령은 망련결, 경로표, 망대면부상태등을 종합적으로 확인할수 있는 망도구입니다. 현재 붉은별봉사기에 설정되여있는 경로조종표를 확인할수 있는 지령입니다.

앞에서 설명한 router 지령도 경로조종표를 확인할수 있지만 netstat 지령을 리용하면 경로조종표뿐아니라 다음과 같은 다양한 정보들을 얻을수 있습니다.

먼저 netstat 지령에서 사용하는 선택항목들중에서 가장 많이 사용하는 선택항목들을 봅니다.

- a : --all 과 같으며 listen 되는 소케트정보와 listen 되지 않는 소케트정보 모두를 보여줍니다.
- n : --numeric 와 같으며 10 진수로 결과를 보여줍니다.
- r : --route 와 같으며 설정된 경로기정보를 보여줍니다.
- p : program 과 같으며 실행되고 있는 매 프로그람과 PID 정보를 보여줍니다.
- i : --interface=iface 와 같으며 모든 망대면부정보를 보여줍니다.

- c : --continuous 와 같으며 netstat 결과를 련속적으로 보여줍니다.
- l : --listening 과 같으며 현재 listen 되고 있는 소케트정보를 보여줍니다.
- s : --statistics 와 같으며 매 규약에 대한 사용자식별자정보를 보여줍니다.

먼저 nr 정보를 사용하면 봉사기에 설정되여 있는 경로표정보를 확인할수 있습니다.

```
[root@localhost profile.d]# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
172.29.88.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
172.29.88.0     0.0.0.0         255.255.248.0   U         0 0          0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth0
0.0.0.0         172.29.88.1     0.0.0.0         UG        0 0          0 eth0
[root@localhost profile.d]# █
```

다음은 –s 선택항목을 사용하면 사용가능한 통신규약들에 대한 통사용자식별자보를 확인할수 있습니다. 이 통신규약에 대한 확인을 한 후에는 봉사기보안과 관련하여 불필요한 통신규약들은 정지하여 합니다.

```
[root@localhost profile.d]# netstat -s
Ip:
    92044 total packets received
    148 with invalid headers
    42394 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    49486 incoming packets delivered
    16474 requests sent out
    12 reassemblies required
    3 packets reassembled ok
    24 fragments received ok
Icmp:
    8570 ICMP messages received
    0 input ICMP message failed.
    ICMP input histogram:
        destination unreachable: 2397
        timeout in transit: 9
        echo requests: 3074
        echo replies: 3090
    5465 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 2391
```

또한 현재 응답하고 있는 매 포구들의 정보를 확인하려면 다음과 같이 합니다. 현재 열려있는 포구를 확인 한 후에 만약 봉사기관리자 자신이 모르는 포구가 있다면 보안점검을 해보아야 합니다. 해킹을 당했을경우에는 알려지지 않은 포구를 사용하는 경우가 있기때문입니다.

```
[root@localhost profile.d]# netstat -an |grep LISTEN
tcp        0      0 0.0.0.0:32768               0.0.0.0:*                   LIST
EN
tcp        0      0 0.0.0.0:3306                0.0.0.0:*                   LIST
EN
tcp        0      0 0.0.0.0:139                 0.0.0.0:*                   LIST
EN
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LIST
EN
tcp        0      0 0.0.0.0:10000               0.0.0.0:*                   LIST
EN
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LIST
EN
tcp        0      0 0.0.0.0:15000               0.0.0.0:*                   LIST
EN
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LIST
EN
tcp        0      0 0.0.0.0:7741                0.0.0.0:*                   LIST
EN
tcp        0      0 0.0.0.0:445                 0.0.0.0:*                   LIST
EN
tcp        0      0 :::80                       :::*                        LIST
EN
tcp        0      0 :::22                       :::*                        LIST
EN
tcp        0      0 :::443                      :::*                        LIST
EN
```

이 지령의 결과로 확인가능한 련결상태표시는 다음과 같은것들이 있습니다.

- LISTEN: 련결이 가능하도록 관련대몬이 실행되고있으며 련결이 가능함을 나타낸다.
- SYS-SENT: 련결을 요청한 상태.
- SYN_RECEIVED: 련결요구에 의한 응답을 준 후에 확인통보문을 기다리고 있는 상태.
- ESTABLISHED: 앞의 세단계련결과정이 모두 완료된 후에 련결이 완료된 상태.
- FIN-WAIT1, CLOSE-WAIT, FIN-WAIT2: 련결완료를 위해 완료요청을 받은 후의 완료과정임.
- CLOSING: 전송된 통보문이 유실된 상태를 나타낸다.
- TIME-WAIT: 련결완료 후에 한동안 유지하고 있는 상태.
- CLOSED: 련결이 완전히 완료됨.
- UNKOWN: 소케트의 상태에 대하여 확인되지 않은 경우.

이번에는 atp 라는 선택항목을 사용하여 현재 응답가능한 (봉사기에서 열려있는) 포구번호들과 매 대몬들 그리고 그 포구를 사용하는 프로그람에 대한 정보를 상세히 점검해볼수 있습니다.

```
[root@localhost profile.d]# netstat -atp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Prog
ram name
tcp        0      0 *:32768                     *:*                         LISTEN      2811/rpc
.statd
tcp        0      0 *:mysql                     *:*                         LISTEN      3172/mys
qld
tcp        0      0 *:netbios-ssn               *:*                         LISTEN      3387/smb
d
tcp        0      0 *:sunrpc                    *:*                         LISTEN      2788/por
tmap
tcp        0      0 *:10000                     *:*                         LISTEN      3558/per
l
tcp        0      0 localhost.localdomain:ipp   *:*                         LISTEN      5179/cup
sd
tcp        0      0 *:15000                     *:*                         LISTEN      3509/per
l
tcp        0      0 localhost.localdomain:smtp  *:*                         LISTEN      3258/sen
dmail: acce
tcp        0      0 *:7741                      *:*                         LISTEN      3405/lis
```

이상과 같이 netstat 지령은 경로표정보를 조회하는 목적외에도 봉사기에서 사용중인 봉사이름에 대한 정보를 얻을수 있습니다. 따라서 보안점검을 할때 많이 사용합니다.

봉사기관리자도 많은 경험을 쌓아야 봉사기의 성능와 효률 그리고 보안이 결정됩니다.

34. tcpdump 를 리용한 TCP 파케트수집 및 파케트자료 관리

tcpdump 는 지정한 망대면부로 송수신되는 자료파케트들의 전체 혹은 머리부등을 수집하여 확인하는 지령입니다.

이 지령의 기본목적은 망과 이써네트의 이상상태를 자료파케트를 통계분석하여 결과를 얻는데 있습니다. 이 지령을 잘 사용하면 수집된 파케트를 분석하여 망이나 봉사기의 응용과정을 분석하는 도구로 사용할수 있지만 악용한다면 크래킹의 도구로 사용될수 있습니다.

즉 통신암호화가 되여 있지 않은 ftp 나 telnet 와 같은 봉사를 리용하여 ID 나 통과암호를 입력하였다면 이 지령으로 파케트수집하여 인차 알아낼수 있습니다. 때문에 가능하다면 통신암호화된 ssh 나 vsftp 를 리용하는것이 좋습니다.

그리고 이 지령을 실행하면 지속적으로 파케트수집을 하기때문에 완료하려면 "^C"를 눌려야 합니다.

1) Ethernet 로 송수신되는 자료파케트 dump.

이 지령을 리용하면 현재 봉사기가 가동중인 이써네트에서 자료파케트의 머리부를 수집하여 볼수 있습니다. 다음과 같이 –i선택항목을 사용하면 수집대상망대면부를 지정할수 있습니다.

```
[root@localhost profile.d]# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
20:06:35.098464 IP 172.29.88.69.netbios-ns > 172.29.95.255.netbios-ns: NBT UDP PACKET(137): REGI
STRATION; REQUEST; BROADCAST
20:06:35.919667 IP 172.29.88.69.netbios-ns > 172.29.95.255.netbios-ns: NBT UDP PACKET(137): REGI
STRATION; REQUEST; BROADCAST
20:06:36.117221 arp who-has 172.29.90.221 tell 172.29.88.66
20:06:36.350635 arp who-has 172.29.93.65 tell 172.29.88.140
20:06:36.676587 arp who-has 172.29.93.1 tell 172.29.88.68
20:06:36.783652 IP 172.29.88.69.netbios-ns > 172.29.95.255.netbios-ns: NBT UDP PACKET(137): REGI
STRATION; REQUEST; BROADCAST
20:06:37.943584 arp who-has 172.29.89.232 tell 172.29.88.8
20:06:37.990961 arp who-has 172.29.92.129 tell 172.29.88.10
20:06:38.617557 IP 172.29.88.69.netbios-ns > 172.29.95.255.netbios-ns: NBT UDP PACKET(137): REGI
STRATION; REQUEST; BROADCAST
20:06:39.459114 IP 172.29.88.69.netbios-ns > 172.29.95.255.netbios-ns: NBT UDP PACKET(137): REGI
STRATION; REQUEST; BROADCAST
20:06:39.759356 arp who-has 172.29.89.233 tell 172.29.88.8
20:06:40.303174 IP 172.29.88.69.netbios-ns > 172.29.95.255.netbios-ns: NBT UDP PACKET(137): REGI
STRATION; REQUEST; BROADCAST

12 packets captured
12 packets received by filter
0 packets dropped by kernel
[root@localhost profile.d]# █
```

2) 특정이써네트로 송수신되는 파케트들을 화일로 보관.

다음은 망대면부로 송수신되는 파케트들을 수집하여 화일로 보관하고 확인하는 방법에 대하여 봅니다. 즉 tcpdump 지령에 –i선택항목 다음에 대상 망대면부를 지정하고 –w 선택항목 다음에는 수집된 파케트를 보관할 화일이름을 임의로 줍니다. 파케트수집을 완료하려면 “^C”를 누른다. 그리고 ls 지령으로 확인합니다.

```
[root@localhost profile.d]# tcpdump -i eth0 -w tcpdump.txt
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
13 packets captured
13 packets received by filter
0 packets dropped by kernel
[root@localhost profile.d]# ls -l
검사합 132
-rwxr-xr-x  1 root root  107  2007  4월 23 10:20 bokemcryptofs.sh
-rwxr-xr-x  1 root root  720  2007  4월 13 06:52 colorls.csh
-rwxr-xr-x  1 root root  713  2007  4월 13 06:52 colorls.sh
-rwxr-xr-x  1 root root  192  2007  3월 26 10:54 glib2.csh
-rwxr-xr-x  1 root root  190  2007  3월 26 10:54 glib2.sh
-rw-r--r--  1 root root   74  2008 12월  9 09:24 java.sh
-rw-r--r--  1 root root   74  2008 12월  9 09:24 java.sh~
-rwxr-xr-x  1 root root   78  2007  4월 21 14:21 kde.csh
-rwxr-xr-x  1 root root   74  2007  4월 21 14:21 kde.sh
-rwxr-xr-x  1 root root 2182  2007  4월 22 10:11 lang.csh
-rwxr-xr-x  1 root root 2470  2007  4월 22 10:11 lang.sh
-rwxr-xr-x  1 root root  122  2004  6월 16 09:20 less.csh
-rwxr-xr-x  1 root root  108  2004  6월 16 09:20 less.sh
-rwxr-xr-x  1 root root   51  2007  8월 17 04:21 mc.csh
-rwxr-xr-x  1 root root   45  2007  8월 17 04:21 mc.sh
-rw-r--r--  1 root root 1108  2009  5월 14 20:14 tcpdump.txt
-rw-r--r--  1 root root  146  2008 12월  9 09:31 tomcat.sh
-rw-r--r--  1 root root  135  2008 12월  9 09:18 tomcat.sh~
-rwxr-xr-x  1 root root  170  2004  8월  7 18:22 which-2.sh
[root@localhost profile.d]#
```

다음 선택항목 –r는 보관된 화일을 본문방식으로 보관하는 선택항목입니다.

```
[root@localhost profile.d]# tcpdump -r tcpdump.txt
reading from file tcpdump.txt, link-type EN10MB (Ethernet)
20:14:48.275197 arp who-has 172.29.93.97 tell 172.29.88.68
20:14:50.502709 arp who-has 172.29.91.61 tell 172.29.88.66
20:14:50.849576 arp who-has 172.29.92.223 tell 172.29.88.10
20:14:51.240572 IP 172.29.88.166.netbios-ns > 172.29.88.255.netbios-ns: NBT UDP PACKET(137): QUE
RY; REQUEST; BROADCAST
20:14:51.854263 arp who-has 172.29.92.214 tell 172.29.88.109
20:14:51.944398 arp who-has 172.29.90.71 tell 172.29.88.8
20:14:52.052877 IP 172.29.88.166.netbios-ns > 172.29.88.255.netbios-ns: NBT UDP PACKET(137): QUE
RY; REQUEST; BROADCAST
20:14:53.269830 arp who-has 172.29.93.98 tell 172.29.88.68
20:14:55.082213 arp who-has 172.29.91.62 tell 172.29.88.66
20:14:55.545877 arp who-has 172.29.92.224 tell 172.29.88.10
20:14:57.587676 arp who-has 172.29.90.72 tell 172.29.88.8
20:14:57.617376 arp who-has 172.29.88.69 tell 172.29.88.68
20:14:57.786561 IP 172.29.88.166.netbios-ns > 172.29.88.255.netbios-ns: NBT UDP PACKET(137): QUE
RY; REQUEST; BROADCAST
[root@localhost profile.d]# _
```

3) 특정이써네트에서 지정한 개수만큼 망의 파케트수집.

tcpdump 지령에서 –i선택항목을 사용하면 수집하려는 망대면부를 지정하고 –c 선택항목 다음에 수집하려는 파케트의 개수를 지정하면 지정된 개수만큼 파케트를 수집을 합니다.

4) 봉사기의 특정포구로 송수신되는 모든 파케트를 확인

tcpdump 지령을 리용하면 파케트머리부만이 아니라 파케트 전체를 수집할 수 있습니다. 아래의 지령을 사용하면 특정 IP 주소의 봉사기로 특정포구를 리용하는 모든 파케트를 수집하여 화일로 보관할수 있습니다.

```
[root@localhost profile.d]# tcpdump -w tcpdump.log -s 1500 tcp port 80 and host 172.29.88.10
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1500 bytes
336 packets captured
336 packets received by filter
0 packets dropped by kernel
[root@localhost profile.d]# █
```

이 지령의 의미는 다음과 같습니다.

-w tcpdump.log: 결과를 화일로 보관합니다.

-s 1 500: 수집할 파케트의 길이로서 1 500 바이트는 파케트의 전체길이를 의미하므로 모든 파케트를 수집하게 됩니다.

tcp port 80: 대상 통신규약과 포구를 지정한것으로서 tcp 포구 80 번으로 송수신되는 파케트를 수집합니다.

host 172.29.88.10: 172.29.88.10 봉사기와 송수신되는 자료를 대상으로 수집합니다.

다음은 우에서 수집한 tcpdump.log 화일의 내용을 ASCII 코드로 확인하는 방법입니다.

```
[root@localhost profile.d]# tcpdump -Xqnr tcpdump.log
reading from file tcpdump.log, link-type EN10MB (Ethernet)
20:36:44.319030 IP 172.29.1.7.http > 172.29.88.10.2998: tcp 0
        0x0000:  4500 0030 0000 4000 3d06 8c7c ac1d 0107  E..0..@.=..|....
        0x0010:  ac1d 580a 0050 0bb6 d45f 33e7 ee3a 9114  ..X..P..._3..:..
        0x0020:  7012 16d0 2757 0000 0204 05b4 0101 0402  p...'W..........
20:36:44.320123 IP 172.29.1.7.http > 172.29.88.10.2998: tcp 0
        0x0000:  4500 0028 a146 4000 3d06 eb3d ac1d 0107  E..(.F@.=..=....
        0x0010:  ac1d 580a 0050 0bb6 d45f 33e8 ee3a 91da  ..X..P..._3..:..
        0x0020:  5010 1920 5105 0000 0000 0000 0000       P...Q.........
20:36:44.373777 IP 172.29.1.7.http > 172.29.88.10.2998: tcp 1460
        0x0000:  4500 05dc a147 4000 3d06 e588 ac1d 0107  E....G@.=.......
        0x0010:  ac1d 580a 0050 0bb6 d45f 33e8 ee3a 91da  ..X..P..._3..:..
        0x0020:  5010 1920 47b1 0000 4854 5450 2f31 2e31  P...G...HTTP/1.1
        0x0030:  2032 3030 204f 4b0d 0a44 6174 653a 2054  .200.OK..Date:.T
        0x0040:  6875 2c20 3134 204d 6179 2032 3030 3920  hu,.14.May.2009.
```

우와 같은 내용을 분석해보면 우리가 사용하고 있는 인터네트환경이 얼마나 취약한가하는것을 느낄수 있습니다.

35. 마지막 등록가입접속확인

- 체계의 매개 사용자식별자의 최근 접속정보를 확인하는 lastlog

lastlog 는 /etc/passwd 화일에 정의되여 있는 모든 사용자식별자의 최근 접속정보를 확인하는 지령입니다.

주로 봉사기의 보안점검을 위하여 필수적으로 확인해 보아야 하는 지령입니다. 간단히 lastlog 라고 하면 모든 사용자식별자의 마지막접속정보를 출력합니다. 봉사기관리자라면 출력되는 정보만을 확인하는것도 중요하지만 이 정보가 어떤 환경에서 출력되였고 또한 그 결과를 어떤 의미로 해석해야 하는가라는 단계까지 분석할수 있어야 능력있는 봉사기관리자라고 말할수 있습니다.

사용형식: lastlog [-u 사용자식별자명][-t 날자]

lastlog 는 /var/log/lastlog 화일의 정보에 저장된 정보를 참조하여 결과를 출력합니다.

/var/log/lastlog 화일은 2 진화일로 되여있기때문에 cat 나 vi 등의 일반편집기로써 확인할수 없습니다. 따라서 lastlog 지령으로 간단히 확인합니다. 참고로 /var/log/lastlog 화일에는 매 사용자식별자의 최근 접속정보가 기록되는 화일입니다.

또한 /usr/include/lastlog.h 화일에 정의된 형식으로 /var/log/lastlog 에 보관됩니다. /usr/include/lastlog.h 화일을 봅시다.

```
# cat /usr/include/lastlog.h
#include <utmp.h>
```

즉 /var/log/lastlog 화일에 보관되는 형식은 /usr/include/utmp.h 화일에 지정된 형식을 사용한다는것을 알수 있습니다.

- 체계 매 사용자식별자의 최근 접속정보확인.

간단히 lastlog 라고만 하면 봉사기의 모든 사용자식별자에 대한 최근 접속정보를 확인할수 있습니다.

```
[root@localhost init.d]# lastlog
Username         Port     From             Latest
root             :0                        금  5월 15 12:20:28 +0900 2009
bin                                        **한번도 가입한적이 없습니다.**
daemon                                     **한번도 가입한적이 없습니다.**
adm                                        **한번도 가입한적이 없습니다.**
lp                                         **한번도 가입한적이 없습니다.**
sync                                       **한번도 가입한적이 없습니다.**
shutdown                                   **한번도 가입한적이 없습니다.**
halt                                       **한번도 가입한적이 없습니다.**
mail                                       **한번도 가입한적이 없습니다.**
news                                       **한번도 가입한적이 없습니다.**
uucp                                       **한번도 가입한적이 없습니다.**
operator                                   **한번도 가입한적이 없습니다.**
games                                      **한번도 가입한적이 없습니다.**
gopher                                     **한번도 가입한적이 없습니다.**
ftp                                        **한번도 가입한적이 없습니다.**
nobody                                     **한번도 가입한적이 없습니다.**
dbus                                       **한번도 가입한적이 없습니다.**
vcsa                                       **한번도 가입한적이 없습니다.**
nscd                                       **한번도 가입한적이 없습니다.**
rpm                                        **한번도 가입한적이 없습니다.**
haldaemon                                  **한번도 가입한적이 없습니다.**
netdump                                    **한번도 가입한적이 없습니다.**
sshd                                       **한번도 가입한적이 없습니다.**
rpc                                        **한번도 가입한적이 없습니다.**
```

"**한번도 가입한적이 없습니다.**" (**never logged in**)는 해당 사용자식별자가 생성된 이후부터 지금까지 한번도 봉사기에 접속한 적이 없다는것을 의미합니다. 만약 어떤 사용자식별자가 어느날 접속했다는 정보가 표시된다면 의심해야 합니다. 어떤 특정사용자식별자의 최근 접속정보를 확인하려한다면 선택항목 –u와 함께 사용합니다.

```
[root@localhost profile.d]# lastlog -u bible
Username         Port     From             Latest
bible            pts/1    172.29.88.30     금  5월 15 16:35:36 +0900 2009
[root@localhost profile.d]# █
```

우의 결과는 bible이란 사용자식별자가 2009년 5월 15일 16시 35분경에 172.29.88.30에서 마지막으로 접속했음을 알수있습니다.

- 지정한 최근날자까지의 체계접속정보확인

Lastlog지령은 최근 몇일까지의 마지막접속정보를 확인할수 있습니다. 이를 확인하기 위해서는 "lastlog –t 30"을 입력합니다. 이 지령은 최근 30일까지의 접속정보를 확인한것입니다.

```
[root@localhost profile.d]# lastlog -t 30
Username         Port     From             Latest
root             :0                        금  5월 15 12:20:28 +0900 2009
bible            pts/1    172.29.88.30     금  5월 15 16:35:36 +0900 2009
[root@localhost profile.d]# █
```

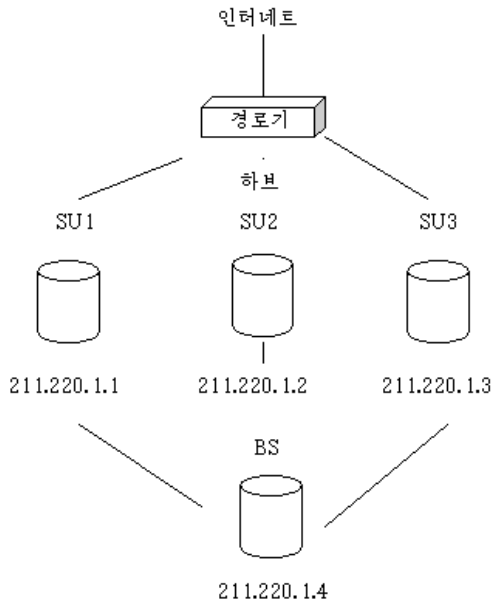
36. 여벌복사봉사기구축

《붉은별》봉사기용체계 3.0 를 비롯한 거의 모든 봉사기에서 여벌복사는 필수적이라고 할수 있습니다. 여기서는 rsync 와 cron 을 리용하여 원격으로 여벌복사하는 방법에 대하여 설명합니다.

여벌복사방법을 설명하기 위하여 다음과 같은 가정을 합니다. 여벌복사봉사기가 각각 SU1, SU2, SU3 이 있고 1 대의 여벌복사봉사기(BS)가 있다고 합시다. 이 경우에 여벌복사봉사기들 자체에서 주기적으로 여벌복사하도록 cron 을 가지고 설정하고 각각의 봉사기에서 여벌복사된 자료들을 여벌복사봉사기로 지정된 시간에 원격으로 자동여벌복사되게 설정합니다.

1) 873 포구를 통한 rsync 여벌복사

rsync 는 원래 자료동기화에 사용되는것이지만 할용여하에 따라서 여벌복사를 수행하는 훌륭한 도구로도 리용될수 있습니다. rsync 는 몇대의 웨브봉사기에 부하를 분산하기 위해 remote sync 작업을 수행하기 위한 목적으로 만들어진것입니다.

rsync 의 man 페지를 보면 수많은 선택항목들에 대하여 설명하고 있는데 봉사기관리자가 이런 rsync 를 어떻게 사용하는가에 따라서 웨브봉사기자료동기화라든가, 여벌복사이라든가하는 작업들을 원하는데로 수행할수 있습니다. 우선 여기서 구축하게될 rsync 를 리용한 여벌복사흐름도를 봅시다.

rsync는 여벌복사대상봉사기와 여벌복사봉사기에 모두 설치되여있어야 합니다. 여벌복사작업은 다음의 단계로 진행합니다.

첫째, SU1, SU2, SU3봉사기들 자체로 cron에 의한 여벌복사을 수행하며 매개의 등록부에 보관됩니다. 이 작업은 매개의 국부봉사기에 주기적으로 (일별, 주별)자동여벌복사되여 특정한 등록부에 보관됩니다. 이것을 국부여벌복사이라고 합니다.

둘째, BS에서 SU1, SU2, SU3봉사기에 여벌복사되여 있는 자료들을 망을 통해 가져오게 됩니다. 이 작업은 BS봉사기의 cron에 의해 수행되며 주기적인(일별, 주별, 월별)작업수행이 가능하며 여기서는 매일 새벽 6시에 자료를 가져오도록 설정합니다.

망여벌복사의 개념은 매우 간단합니다. 그러나 이를 구성하기 위해서는 조작체계에 대한 리해가 필요하며 특히 cron작업과 rsync에 의한 작업들에 대한 개념과 리해가 필요합니다. 그러면 여벌복사대상봉사기들과 여벌복사봉사기에서 설정되여야 할 내용에 대하여 봅니다.

2) 여벌복사대상봉사기들의 설정내용

여기서 설정하는 내용들은 여벌복사대상봉사기들에 모두 동일하게 설정되여야 할 내용들입니다. 여기서는 어느 한 봉사기의 설정에 대하여 봅니다.

a. 우선 여벌복사대상봉사기의 보안조작체계보안설정을 해제해야 합니다.

보안설정을 해제하자면 보안관리자권한을 획득해야 합니다.

《붉은별》봉사기용체계 3.0 에서는 보안을 위하여 관리자등급을 다음과 같이 할당하였습니다.

보안관리자: secadm_r ---------높다

체계관리자: sysadm_r

Root 관리자: staff_r

일반사용자: user_r------------낮다

붉은별체계를 설치했을 때 국부체계에서는 기정적으로 sysadm_r 사용자가 된다

원격으로 가입했을 때는 staff_r 사용자가 됩니다.

때문에 다음과 같이 보안관리자권한을 획득해야 합니다.

```
-bash-4.1# newrole -r secadm_r
암호:
[root@c5 /]# id -Z
root:secadm_r:secadm_t:s0-s15:c0.c1023
[root@c5 /]#
```

여기서 newrole 은 지령이고 –r 는 파라메터이며 secadm_r 는 사용자명입니다.

통과암호는 root 통과암호를 입력합니다.

#id –Z 지령은 지령의 실행여부를 확인하는 지령입니다.

다음 보안 보안조작체계를 해제합니다.

```
[root@c5 /]# setenforce 0
[root@c5 /]# getenforce
Permissive
[root@c5 /]#
```

#setenforce 0 이면 보안조작체계를 비활성화, 1 이면 활성화합니다.

getenforce 지령은 우의 지령실행여부를 확인하는 지령으로서 결과가 Permissive 이면 실행이 정상이다는 뜻입니다.

b. 다음 /etc/services 화일안에서 rsync 873 포구를 확인해야 합니다. 왜냐면 rsync 작업은 873 포구를 리용하기 때문입니다. 따라서 가장 기본적인 포구사용이 가능해야 하므로 이 포구가 열려있는지를 /etc/services 화일에서 확인합니다. 일반적으로 봉사기설정을 하면 기본보안설정을 하게 되는데 이런 보안설정중의 하나로/etc/services 화일안의 불필요한 포구들은 모두 설명처리하게 됩니다. 만약 이부분이 설명처리되였다면 설명을 해제해주어야 합니다.

```
[root@localhost ~]# cat /etc/services | grep 873
rsync           873/tcp                         # rsync
rsync           873/udp                         # rsync
fjmpjps         1873/tcp                # Fjmpjps
fjmpjps         1873/udp                # Fjmpjps
fagordnc        3873/tcp                # fagordnc
fagordnc        3873/udp                # fagordnc
dtp-net         8732/udp                # DASGIP Net Services
ibus            8733/tcp                # iBus
ibus            8733/udp                # iBus
dxspider        8873/tcp                # dxspider linking protocol
dxspider        8873/udp                # dxspider linking protocol
[root@localhost ~]#
```

c. xinetd 설정.

이 화일은 /etc/xinetd.d 등록부안에 rsync 라는 화일로 존재합니다. 이 화일에서 설치한후 disable 파라메터가 yes 로 되여 있습니다. 이것을 no 로 수정해서 이 봉사를 허가해주어야 합니다.

```
# cat /etc/xinetd.d/rsync
service rsync
{
        disable=no
        socket_type=stream
        wait =no
        user=root
        server=/usr/local/bin/rsync
        server_arge=--daemon
```

log_on_failure+=USREID

}

이 화일을 수정하였다면 xinetd 대몬을 재시동해야 합니다.

service xinetd restart

이 화일은 어떤 내용을 여벌복사할것인가, 그리고 rsync 로 접근을 허용하는 봉사기들에 대한 설정을 합니다. 이 화일의 설정내용들에 대한 의미는 아래표와 같습니다.

d. crontab 의 설정

crond 프로그람은 설정된 지령을 주기적으로 실행하는 데몬으로서 구성화일을 다음과 같이 구성할수 있습니다.

```
[root@c5 /]# crontab -e
```

이 지령을 실행하면 vi 편집기기 기동하면서 /var/spool/cron/root 화일이 현시됩니다.

```
9 12 * * * /etc/beam/cron/tempdelete.pl
5 17 * * * rsync -avz localhost:/var/lib/mysql /dev/sda6/var/lib/mysql
```

A 건반을 누르면 편집상태로 들어간다. 다음 두번째행을 입력합니다.

두번째행의 의미는 매일 17 시 5 분에 자료기지화일들을 다른 하드디스크에 보관하라는 뜻입니다. 편집상태에서 탈퇴하려면 esc 건을 누르고 shiht+:을 누른 상태에서 wq 를 누르고 enter 건을 누르면 편집된 내용을 보관하고 vi편집기에서 탈퇴합니다.이러게 3 대의 봉사기자료들을 국부체계에 여벌복사합니다.

2) 여벌복사봉사기(BS)의 설정.

여기서는 여벌복사봉사기에서 설정해야 할 내용들을 설명합니다.

우의 과정과 모두 같고 crontab –e 지령을 입력했을때 나오는 편집내용이 좀 차이난다.

```
9 12 * * * /etc/beam/cron/tempdelete.pl
0 20 * * * rsync -avz 211.220.1.1:/var/lib/mysql /mnt/server1-backup
0 21 * * * rsync -avz 211.220.1.2:/var/lib/mysql /mnt/server2-backup
0 22 * * * rsync -avz 211.220.1.3:/var/lib/mysql /mnt/server3-backup
```

–avz 선택항목의 의미는 다음과 같습니다.

-a: achive mode로서 기존의 속성 및 권한, 소유권등의 설정내용을 그대로 유지.

-v: verbose mode로서 작업내용을 상세하게 보여줍니다.

-z: 전송속도를 높이기 위해 압축을 진행하여 전송합니다.

다음의 cron 대몬을 다음과 같이 재기동 해줍니다.

```
[root@dell-rss etc]# service crond restart
crond를 중지시키고 있습니다:                    [  확인  ]
crond를 시작하고 있습니다:                      [  확인  ]
[root@dell-rss etc]#
```